(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平１０－３２７１４２

(43)公開日　平成１０年（１９９８）１２月８日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
H04L 9/14			H04L 9/00	641	
G06K 17/00			G06K 17/00	T	
G09C 1/00	660		G09C 1/00	660 A	
H04L 9/32			H04L 9/00	675 A	

審査請求　未請求　請求項の数２５　ＯＬ　（全２１頁）

(21)出願番号　特願平９－１１０８８９

(22)出願日　平成９年（１９９７）４月２８日

(31)優先権主張番号　特願平９－７３２０５

(32)優先日　平９（１９９７）３月２６日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　０００００２１８５
ソニー株式会社
東京都品川区北品川６丁目７番３５号

(72)発明者　日下部　進
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

(72)発明者　石橋　義人
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

(72)発明者　高田　昌幸
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

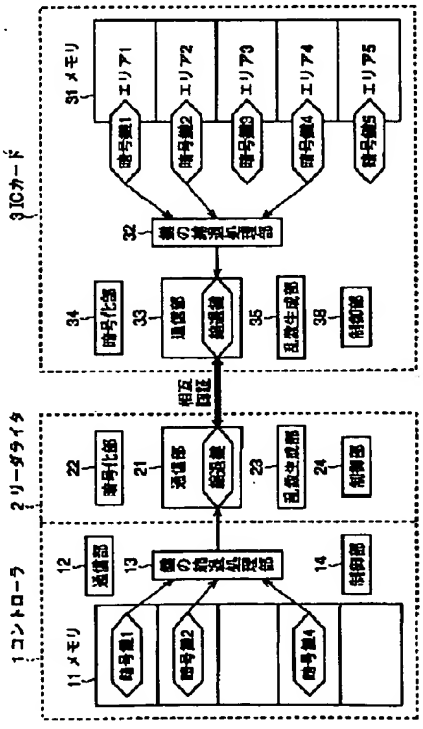
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】認証システムおよび方法、並びに認証装置および方法

(57)【要約】

【課題】　複数の暗号鍵を用いて認証を行う場合における認証時間を短くする。

【解決手段】　ＩＣカード３のメモリ３１のエリア１乃至エリア５のうち、各エリアアクセスするのに、それぞれ暗号鍵１乃至暗号鍵５が必要である場合、アクセスする複数のエリアを、リーダライタ２からＩＣカード３に通知し、そのエリアに対応する複数の暗号鍵（例えば暗号鍵１、暗号鍵２、および暗号鍵４）を読み出し、縮退処理部３２で、それらから１つの縮退鍵を生成させる。また、リーダライタ２の乱数生成部２３で生成した乱数をＩＣカード３に転送し、暗号化部３４で、縮退鍵を用いて暗号化させる。リーダライタ２は、ＩＣカード３から、この暗号化された乱数の転送を受け、縮退鍵を用いて復号化し、復号化した乱数と発生した乱数とが等しければ、ＩＣカード３が適正なものとであるとする。



1

【特許請求の範囲】

【請求項１】　第１の装置と第２の装置との間で認証処理を行う認証システムにおいて、

前記第１の装置は、

複数の鍵を記憶する第１の記憶手段と、

前記第１の記憶手段に記憶されている複数の前記鍵のうちの任意の数の鍵から、１つの認証鍵を生成する第１の生成手段と、

前記第２の装置との間で通信を行う第１の通信手段と、

を備え、

前記第２の装置は、

複数の鍵を記憶する第２の記憶手段と、

前記第２の記憶手段に記憶されている複数の前記鍵のうちの任意の数の鍵から、１つの認証鍵を生成する第２の生成手段と、

前記第１の装置との間で通信を行う第２の通信手段とを備え、

前記第１の装置と第２の装置の一方は、前記認証鍵を用いて暗号化を行う暗号化手段を備え、

前記第１の装置と第２の装置の他方は、前記暗号化手段により暗号化されたデータを前記認証鍵を用いて復号化する復号化手段を備えることを特徴とする認証システム。

【請求項２】　前記第１の装置と第２の装置の一方は、他方に対して、そこに記憶されている複数の前記鍵のうちの任意の数の鍵から、対応する１つの認証鍵を生成するのに必要な情報を通知する通知手段をさらに備え、

前記第１の装置と第２の装置の他方は、前記通知手段により通知された情報に対応して前記認証鍵を生成することを特徴とする請求項１に記載の認証システム。

【請求項３】　前記第１の装置と第２の装置の少なくとも一方は、乱数を生成する乱数生成手段を備え、

前記暗号化手段は、前記乱数生成手段で生成された乱数を暗号化し、

前記復号化手段は、暗号化された前記乱数を復号化することを特徴とする請求項１に記載の認証システム。

【請求項４】　前記第２の装置は、複数の前記鍵に対応する複数の情報記録領域を有することを特徴とする請求項１に記載の認証システム。

【請求項５】　第１の装置と第２の装置との間で認証処理を行う認証方法において、

前記第１の装置は、

複数の鍵を記憶する第１の記憶ステップと、

前記第１の記憶ステップで記憶された複数の前記鍵のうちの任意の数の鍵から、１つの認証鍵を生成する第１の生成ステップと、

前記第２の装置との間で通信を行う第１の通信ステップと、

を備え、

前記第２の装置は、

2

複数の鍵を記憶する第２の記憶ステップと、

前記第２の記憶ステップで記憶された複数の前記鍵のうちの任意の数の鍵から、１つの認証鍵を生成する第２の生成ステップと、

前記第１の装置との間で通信を行う第２の通信ステップとを備え、

前記第１の装置と第２の装置の一方は、前記認証鍵を用いて暗号化を行う暗号化ステップを備え、

前記第１の装置と第２の装置の他方は、前記暗号化ステップで暗号化されたデータを前記認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする認証方法。

【請求項６】　他の装置との間で認証処理を行う認証装置において、

前記他の装置との間で通信を行う通信手段と、

複数の鍵を記憶する記憶手段と、

前記記憶手段に記憶されている複数の前記鍵のうちの任意の数の鍵から、１つの認証鍵を生成する生成手段と、

前記他の装置に対して、前記他の装置に記憶されている複数の前記鍵のうちの任意の数の鍵から、対応する１つの認証鍵を生成するのに必要な情報と、前記認証鍵を用いて暗号化するデータを通知する通知手段と、

前記他の装置が前記認証鍵を用いて暗号化したデータを、前記認証鍵を用いて復号化する復号化手段とを備えることを特徴とする認証装置。

【請求項７】　前記通知手段は、前記暗号化するデータとして、乱数を通知することを特徴とする請求項６に記載の認証装置。

【請求項８】　他の装置との間で認証処理を行う認証方法において、

前記他の装置との間で通信を行う通信ステップと、

複数の鍵を記憶する記憶ステップと、

前記記憶ステップで記憶された複数の前記鍵のうちの任意の数の鍵から、１つの認証鍵を生成する生成ステップと、

前記他の装置に対して、前記他の装置に記憶されている複数の前記鍵のうちの任意の数の鍵から、対応する１つの認証鍵を生成するのに必要な情報を通知する通知ステップと、

前記他の装置が前記認証鍵を用いて暗号化したデータを、前記認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする認証方法。

【請求項９】　他の装置との間で認証処理を行う認証装置において、

前記他の装置との間で通信を行う通信手段と、

複数の鍵を記憶する記憶手段と、

前記他の装置から通知された情報に基づいて、前記記憶手段に記憶されている複数の前記鍵のうちの任意の数の鍵から、１つの認証鍵を生成する生成手段と、前記他の装置から通知されたデータを、前記認証鍵を用いて暗号

3

化する暗号化手段とを備えることを特徴とする認証装置。

【請求項１０】　複数の前記鍵に対応する複数の情報記録領域をさらに有することを特徴とする請求項９に記載の認証装置。

【請求項１１】　他の装置との間で認証処理を行う認証方法において、

前記他の装置との間で通信を行う通信ステップと、

複数の鍵を記憶する記憶ステップと、

前記他の装置から通知された情報に基づいて、前記記憶ステップで記憶された複数の前記鍵のうちの任意の数の鍵から、１つの認証鍵を生成する生成ステップと、

前記他の装置から通知されたデータを、前記認証鍵を用いて暗号化する暗号化ステップとを備えることを特徴とする認証方法。

【請求項１２】　第１の装置と第２の装置との間で認証処理を行う認証システムにおいて、

前記第１の装置は、

自己に割り当てられた鍵を記憶するとともに、所定の共通データと、前記第２の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する第１の記憶手段と、

前記第１の記憶手段に記憶されている前記鍵と、前記個別データとから、認証鍵を生成する第１の生成手段と、

前記他の装置が対応する前記認証鍵を生成するのに必要な情報を通知する通知手段と、

前記第２の装置との間で通信を行う第１の通信手段とを備え、

前記第２の装置は、

複数の鍵と前記共通データを記憶する第２の記憶手段と、

前記第２の記憶手段に記憶されている複数の前記鍵のうち、前記第１の装置の通信手段からの通知に対応するものと、前記共通データとから、前記認証鍵を生成する第２の生成手段と、

前記第１の装置との間で通信を行う第２の通信手段とを備え、

前記第１の装置と第２の装置の一方は、前記認証鍵を用いて暗号化を行う暗号化手段を備え、

前記第１の装置と第２の装置の他方は、前記暗号化手段により暗号化されたデータを前記認証鍵を用いて復号化する復号化手段を備えることを特徴とする認証システム。

【請求項１３】　前記認証鍵は、第１の認証鍵と第２の認証鍵で構成され、前記第１の生成手段は、前記第１の記憶手段に記憶されている、自己に割り当てられている前記鍵と、前記個別データとから、前記第１の認証鍵を生成し、自己に割り当てられている前記鍵と、前記第１の認証鍵を用いて前記第２の認証鍵を生成し、

前記第２の生成手段は、前記第２の記憶手段に記憶されている複数の前記鍵のうち、前記第１の装置の通知手段からの通知に対応するものと、前記共通データとから、前記第１の認証鍵を生成し、前記第１の認証鍵と、前記第２の記憶手段に記憶されている複数の前記鍵のうち、前記第１の装置の通知手段からの通知に対応するものを用いて前記第２の認証鍵を生成し、

前記第１の装置と第２の装置は、いずれも前記暗号化手段と復号化手段を備え、

前記第１の装置と第２の装置の一方は、乱数を生成する乱数生成手段をさらに備え、

前記第１の装置と第２の装置の一方の暗号化手段は、前記乱数生成手段で生成された乱数を前記第１の認証鍵を用いて暗号化し、

前記第１の装置と第２の装置の他方の復号化手段は、前記第１の装置と第２の装置の一方の暗号化手段により暗号化された前記乱数を前記第１の認証鍵を用いて復号化し、

前記第１の装置と第２の装置の他方の暗号化手段は、前記第１の装置と第２の装置の他方の復号化手段により復号化された前記乱数を、前記第２の認証鍵を用いて暗号化し、

前記第１の装置と第２の装置の一方の復号化手段は、前記第１の装置と第２の装置の他方の暗号化手段により暗号化された前記乱数を前記第２の認証鍵を用いて復号化することを特徴とする請求項１２に記載の認証システム。

【請求項１４】　前記第１の装置と第２の装置の一方は、他方から、他方の装置に固有の装置識別番号の送信を受け、

前記第１の装置と第２の装置の他方は、前記第１の記憶手段または第２の記憶手段に、前記装置識別番号をさらに記憶し、

前記第１の装置の第１の生成手段と、前記第２の装置の第２の生成手段は、前記認証鍵を生成するのに、前記装置識別番号をさらに用いることを特徴とする請求項１２に記載の認証システム。

【請求項１５】　前記第１の装置の第１の通信手段は、前記第２の装置の第２の記憶手段に記憶されている複数の前記鍵のうち、所定の第１の鍵を新たな第２の鍵で更新する場合、前記第２の鍵を前記第１の鍵で暗号化した第１の暗号化データと、前記第２の鍵に対して所定の関係にある第３の鍵を前記第１の鍵で暗号化した第２の暗号化データを、更新する前記鍵の鍵識別番号とともに前記第２の装置に送信することを特徴とする請求項１２に記載の認証システム。

【請求項１６】　前記第２の装置は、前記第１の装置の第１の通信手段から送信を受けた、前記第１の暗号化データと第２の暗号化データを、前記鍵識別番号に対応する前記第１の鍵を用いて復号化する第２の復号化手段と、

5

復号化された前記第２の鍵と第３の鍵が所定の関係にあるか否かを判定し、判定結果に対応して前記第１の鍵を前記第２の鍵で更新する更新手段とをさらに備えることを特徴とする請求項１５に記載の認証システム。

【請求項１７】　第１の装置と第２の装置との間で認証処理を行う認証方法において、

前記第１の装置は、

自己に割り当てられた鍵を記憶するとともに、所定の共通データと、前記第２の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する第１の記憶ステップと、

前記第１の記憶ステップで記憶されている前記鍵と、前記個別データとから、認証鍵を生成する第１の生成ステップと、

前記他の装置が対応する前記認証鍵を生成するのに必要な情報を通知する通知ステップと、

前記第２の装置との間で通信を行う第１の通信ステップとを備え、

前記第２の装置は、

複数の鍵と前記共通データを記憶する第２の記憶ステップと、

前記第２の記憶ステップで記憶されている複数の前記鍵のうち、前記第１の装置の通信ステップからの通知に対応するものと、前記共通データとから、前記認証鍵を生成する第２の生成ステップと、

前記第１の装置との間で通信を行う第２の通信ステップとを備え、

前記第１の装置と第２の装置の一方は、前記認証鍵を用いて暗号化を行う暗号化ステップを備え、

前記第１の装置と第２の装置の他方は、前記暗号化ステップにより暗号化されたデータを前記認証鍵を用いて復号化する復号化ステップを備えることを特徴とする認証方法。

【請求項１８】　他の装置との間で認証処理を行う認証装置において、

自己に割り当てられた鍵を記憶するとともに、所定の共通データと、前記他の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する記憶手段と、

前記記憶手段に記憶されている前記鍵と、前記個別データとから、認証鍵を生成する生成手段と、

前記他の装置が対応する前記認証鍵を生成するのに必要な情報を通知する通知手段と、

前記他の装置との間で通信を行う通信手段と、

前記認証鍵を用いて暗号化を行う暗号化手段とを備えることを特徴とする認証装置。

【請求項１９】　前記生成手段は、前記認証鍵を生成するのに、前記他の装置に固有の装置識別番号をさらに用いることを特徴とする請求項１８に記載の認証装置。

【請求項２０】　前記通信手段は、前記他の装置に記憶されている複数の前記鍵のうち、所定の第１の鍵を新た

6

な第２の鍵で更新する場合、前記第２の鍵を前記第１の鍵で暗号化した第１の暗号化データと、前記第２の鍵に対して所定の関係にある第３の鍵を前記第１の鍵で暗号化した第２の暗号化データを、更新する前記鍵の鍵識別番号とともに前記他の装置に送信することを特徴とする請求項１８に記載の認証装置。

【請求項２１】　他の装置との間で認証処理を行う認証方法において、

自己に割り当てられた鍵を記憶するとともに、所定の共通データと、前記他の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する記憶ステップと、

前記記憶ステップで記憶されている前記鍵と、前記個別データとから、認証鍵を生成する生成ステップと、

前記他の装置が対応する前記認証鍵を生成するのに必要な情報を通知する通知ステップと、

前記他の装置との間で通信を行う通信ステップと、

前記認証鍵を用いて暗号化を行う暗号化ステップとを備えることを特徴とする認証方法。

【請求項２２】　他の装置との間で認証処理を行う認証装置において、

複数の鍵と共通データを記憶する記憶手段と、

前記記憶手段に記憶されている複数の前記鍵のうち、前記他の装置からの通知に対応するものと、前記共通データとから、認証鍵を生成する生成手段と、

前記他の装置との間で通信を行う通信手段と、

前記他の装置により暗号化されたデータを前記認証鍵を用いて復号化する復号化手段とを備えることを特徴とする認証装置。

【請求項２３】　前記生成手段は、前記認証鍵を生成するのに、前記他の装置からの通知情報以外に、自己に固有の装置識別番号を用いることを特徴とする請求項２２に記載の認証装置。

【請求項２４】　前記他の装置から、前記記憶手段に記憶されている複数の前記鍵のうち、所定の第１の鍵を新たな第２の鍵で更新するために、前記第２の鍵を前記第１の鍵で暗号化した第１の暗号化データと、前記第２の鍵に対して所定の関係にある第３の鍵を、前記第１の鍵で暗号化した第２の暗号化データを、更新する前記鍵の鍵識別番号とともに送信を受けたとき、前記第１の暗号化データと第２の暗号化データを、更新する前記鍵の鍵識別番号に対応する前記第１の鍵を用いて復号化する第２の復号化手段と、

復号化された前記第２の鍵と第３の鍵が所定の関係にあるか否かを判定し、判定結果に対応して前記第１の鍵を前記第２の鍵で更新する更新手段とをさらに備えることを特徴とする請求項２２に記載の認証装置。

【請求項２５】　他の装置との間で認証処理を行う認証方法において、

複数の鍵と共通データを記憶する記憶ステップと、

前記記憶ステップで記憶されている複数の前記鍵のう

7

ち、前記他の装置からの通知に対応するものと、前記共通データとから、認証鍵を生成する生成ステップと、
前記他の装置との間で通信を行う通信ステップと、
前記他の装置により暗号化されたデータを前記認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、認証システムおよび方法、並びに認証装置および方法に関し、特に、より迅速に、認証を行うことができるようにした、認証システムおよび方法、並びに認証装置および方法に関する。

【０００２】

【従来の技術】図２０は、ＩＣカードにおける、従来の認証システムの構成例を表している。この構成例においては、ＩＣカード１０２とリーダライタ１０１の間で、認証処理を行うようになされている。ＩＣカード１０２は、情報を記憶するためのエリアが、エリア１乃至エリア５の５つのエリアに区分されている。そして、各エリア毎に、それぞれ異なる暗号鍵１乃至暗号鍵５が対応されている。エリアｉをアクセスするには、対応する暗号鍵ｉが必要となる。

【０００３】すなわち、リーダライタ１０１が、ＩＣカード１０２の、例えばエリア１にデータを記録するか、あるいは、そこに記録されているデータを読み出す場合、最初に、相互認証処理が行われる。リーダライタ１０１は、ＩＣカード１０２が記憶している暗号鍵１乃至暗号鍵５と同一の符号鍵１乃至暗号鍵５を予め記憶している。そして、ＩＣカード１０２のエリア１にアクセスする場合には、このエリア１に対応する暗号鍵１を読み出し、これを用いて認証処理を行う。

【０００４】例えば、リーダライタ１０１は、所定の乱数を発生し、この乱数とアクセスすべきエリアの番号１をＩＣカード１０２に通知する。ＩＣカード１０２においては、通知されてきた番号１のエリアに対応する暗号鍵１を読み出し、その暗号鍵１を用いて、通知されてきた乱数を暗号化する。そして、暗号化した乱数を、リーダライタ１０１に通知する。リーダライタ１０１は、この暗号化された乱数を暗号鍵を用いて復号化する。ＩＣカード１０２に通知した乱数と復号化した乱数とが一致していれば、ＩＣカード１０２が適正なものであるとの判定を行う。

【０００５】同様に、ＩＣカード１０２は、所定の乱数を発生し、リーダライタ１０１に出力する。リーダライタ１０１は、暗号鍵１を用いて、この乱数を暗号化し、暗号化した乱数をＩＣカード１０２に通知する。ＩＣカード１０２は、この暗号化された乱数を暗号鍵１を用いて復号化する。そして、復号化された乱数とリーダライタ１０１に通知した乱数とが一致していれば、リーダライタ１０１が適正なリーダライタであると判定する。

8

【０００６】以上の処理は、各エリア毎に行われる。

【０００７】

【発明が解決しようとする課題】このように、従来のシステムにおいては、相互認証処理が、エリア毎に個別に行われるようになされているため、各エリアに、迅速にアクセスすることが困難である課題があった。その結果、例えば、通勤者が、改札口に設けられているゲートを通過する、比較的短い時間の間に、ＩＣカード１０２の所定のエリアにリーダライタ１０１がアクセスし、情報を書き込み、または読み出すことが困難となる課題があった。

【０００８】本発明はこのような状況に鑑みてなされたものであり、より迅速な認証ができるようにするものである。

【０００９】

【課題を解決するための手段】請求項１に記載の認証システムは、第１の装置は、複数の鍵を記憶する第１の記憶手段と、第１の記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する第１の生成手段と、第２の装置との間で通信を行う第１の通信手段と、を備え、第２の装置は、複数の鍵を記憶する第２の記憶手段と、第２の記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する第２の生成手段と、第１の装置との間で通信を行う第２の通信手段とを備え、第１の装置と第２の装置の一方は、認証鍵を用いて暗号化を行う暗号化手段を備え、第１の装置と第２の装置の他方は、暗号化手段により暗号化されたデータを認証鍵を用いて復号化する復号化手段とを備えることを特徴とする。

【００１０】請求項５に記載の認証方法は、第１の装置は、複数の鍵を記憶する第１の記憶ステップと、第１の記憶ステップで記憶された複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する第１の生成ステップと、第２の装置との間で通信を行う第１の通信ステップと、を備え、第２の装置は、複数の鍵を記憶する第２の記憶ステップと、第２の記憶ステップで記憶された複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する第２の生成ステップと、第１の装置との間で通信を行う第２の通信ステップとを備え、第１の装置と第２の装置の一方は、認証鍵を用いて暗号化を行う暗号化ステップを備え、第１の装置と第２の装置の他方は、暗号化ステップで暗号化されたデータを認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする。

【００１１】請求項６に記載の認証装置は、他の装置との間で通信を行う通信手段と、複数の鍵を記憶する記憶手段と、記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する生成手段と、他の装置に対して、他の装置に記憶されている複数の鍵のうちの任意の数の鍵から、対応する１つの認証鍵を生成するのに必要な情報と、認証鍵を用いて暗号化するデ

9

ータを通知する通知手段と、他の装置が認証鍵を用いて暗号化したデータを、認証鍵を用いて復号化する復号化手段とを備えることを特徴とする。

【００１２】請求項８に記載の認証方法は、他の装置との間で通信を行う通信ステップと、複数の鍵を記憶する記憶ステップと、記憶ステップで記憶された複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する生成ステップと、他の装置に対して、他の装置に記憶されている複数の鍵のうちの任意の数の鍵から、対応する１つの認証鍵を生成するのに必要な情報を通知する通知ステップと、他の装置が認証鍵を用いて暗号化したデータを、認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする。

【００１３】請求項９に記載の認証装置は、他の装置との間で通信を行う通信手段と、複数の鍵を記憶する記憶手段と、他の装置から通知された情報に基づいて、記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する生成手段と、他の装置から通知されたデータを、認証鍵を用いて暗号化する暗号化手段とを備えることを特徴とする。

【００１４】請求項１１に記載の認証方法は、他の装置との間で通信を行う通信ステップと、複数の鍵を記憶する記憶ステップと、他の装置から通知された情報に基づいて、記憶ステップで記憶された複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する生成ステップと、他の装置から通知されたデータを、認証鍵を用いて暗号化する暗号化ステップとを備えることを特徴とする。

【００１５】請求項１２に記載の認証システムは、第１の装置は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、第２の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する第１の記憶手段と、第１の記憶手段に記憶されている鍵と、個別データとから、認証鍵を生成する第１の生成手段と、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知手段と、第２の装置との間で通信を行う第１の通信手段とを備え、第２の装置は、複数の鍵と共通データを記憶する第２の記憶手段と、第２の記憶手段に記憶されている複数の鍵のうち、第１の装置の通信手段からの通知に対応するものと、共通データとから、認証鍵を生成する第２の生成手段と、第１の装置との間で通信を行う第２の通信手段とを備え、第１の装置と第２の装置の一方は、認証鍵を用いて暗号化を行う暗号化手段を備え、第１の装置と第２の装置の他方は、暗号化手段により暗号化されたデータを認証鍵を用いて復号化する復号化手段を備えることを特徴とする。

【００１６】請求項１７に記載の認証方法は、第１の装置は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、第２の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する第１の記憶ステップと、第１の記憶ステップで記憶されている鍵と、個別データとから、認証鍵を生成する第１の生成ステップと、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知ステップと、第２の装置との間で通信を行う第１の通信ステップとを備え、第２の装置は、複数の鍵と共通データを記憶する第２の記憶ステップと、第２の記憶ステップで記憶されている複数の鍵のうち、第１の装置の通信ステップからの通知に対応するものと、共通データとから、認証鍵を生成する第２の生成ステップと、第１の装置との間で通信を行う第２の通信ステップとを備え、第１の装置と第２の装置の一方は、認証鍵を用いて暗号化を行う暗号化ステップを備え、第１の装置と第２の装置の他方は、暗号化ステップにより暗号化されたデータを認証鍵を用いて復号化する復号化ステップを備えることを特徴とする。

【００１７】請求項１８に記載の認証装置は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、他の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する記憶手段と、記憶手段に記憶されている鍵と、個別データとから、認証鍵を生成する生成手段と、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知手段と、他の装置との間で通信を行う通信手段と、認証鍵を用いて暗号化を行う暗号化手段とを備えることを特徴とする。

【００１８】請求項２１に記載の認証方法は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、他の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する記憶ステップと、記憶ステップで記憶されている鍵と、個別データとから、認証鍵を生成する生成ステップと、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知ステップと、他の装置との間で通信を行う通信ステップと、認証鍵を用いて暗号化を行う暗号化ステップとを備えることを特徴とする。

【００１９】請求項２２に記載の認証装置は、複数の鍵と共通データを記憶する記憶手段と、記憶手段に記憶されている複数の鍵のうち、他の装置からの通知に対応するものと、共通データとから、認証鍵を生成する生成手段と、他の装置との間で通信を行う通信手段と、他の装置により暗号化されたデータを認証鍵を用いて復号化する復号化手段とを備えることを特徴とする。

【００２０】請求項２５に記載の認証方法は、複数の鍵と共通データを記憶する記憶ステップと、記憶ステップで記憶されている複数の鍵のうち、他の装置からの通知に対応するものと、共通データとから、認証鍵を生成する生成ステップと、他の装置との間で通信を行う通信ステップと、他の装置により暗号化されたデータを認証鍵を用いて復号化する復号化ステップとを備えることを特徴とする。

【００２１】請求項１に記載の認証システムおよび請求

10

項５に記載の認証方法においては、複数の鍵から１つの認証鍵が生成される。そして、この１つの認証鍵を用いて、データが暗号化され、また、復号化される。

【００２２】請求項６に記載の認証装置および請求項８に記載の認証方法においては、複数の鍵を用いて、１つの認証鍵を生成するのに必要な情報が、他の装置に通知される。そして、他の装置で生成された認証鍵を用いて暗号化されたデータが、認証鍵を用いて復号化される。

【００２３】請求項９に記載の認証装置および請求項１１に記載の認証方法においては、他の装置から通知された情報に基づいて、複数の鍵から１つの認証鍵が生成される。そして、生成した認証鍵を用いて、データが暗号化される。

【００２４】請求項１２に記載の認証システムおよび請求項１７に記載の認証方法においては、第１の装置に、自己に割り当てられた鍵と、個別データが記憶されており、これらに対応して認証鍵が生成される。第２の装置では、第１の装置からの通知と、共通データとから、認証鍵が生成される。

【００２５】請求項１８に記載の認証装置および請求項２１に記載の認証方法においては、共通データと、他の装置が保持する所定の数の鍵を用いて生成された個別データが、自己に割り当てられた鍵とともに記憶されている。自己に割り当てられた鍵と、個別データとから、認証鍵が生成される。

【００２６】請求項２２に記載の認証装置および請求項２５に記載の認証方法においては、他の装置からの通知に対応する鍵と、共通データとから、認証鍵が生成される。

【００２７】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００２８】請求項１に記載の認証システムは、第１の装置は、複数の鍵を記憶する第１の記憶手段（例えば、図１のメモリ１１）と、第１の記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する第１の生成手段（例えば、図１の縮退処理部１３）と、第２の装置との間で通信を行う第１の通信手段（例えば、図１の通信部１２）と、を備え、第２の装置は、複数の鍵を記憶する第２の記憶手段（例えば、図１のメモリ３１）と、第２の記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する第２の生成手段（例えば、図１の縮退処理部３２）と、第１の装置との間で通信を行う第２の通信手段（例えば、図１の通信部３３）とを備え、第１の装置と第２の装置の一方（例えば、図１のＩＣカード３）は、認証鍵を用いて暗号化を行う暗号化手段（例えば、図１の暗号化部３４）を備え、第１の装置と第２の装置の他方（例えば、図１のコントローラ１およびリーダライタ２）は、暗号化手段により暗号化されたデータを認証鍵を用いて復号化する復号化手段（例えば、図１の暗号化部２２）とを備えることを特徴とする。

【００２９】請求項２に記載の認証システムは、第１の装置と第２の装置の一方は、他方に対して、そこに記憶されている複数の鍵のうちの任意の数の鍵から、対応する１つの認証鍵を生成するのに必要な情報を通知する通知手段（例えば、図７のステップＳ６）をさらに備え、第１の装置と第２の装置の他方は、通知手段により通知された情報に対応して認証鍵を生成することを特徴とする。

【００３０】請求項３に記載の認証システムは、第１の装置と第２の装置の少なくとも一方は、乱数を生成する乱数生成手段（例えば、図１の乱数生成部２３，３５）を備え、暗号化手段は、乱数生成手段で生成された乱数を暗号化し、復号化手段は、暗号化された乱数を復号化することを特徴とする。

【００３１】請求項６に記載の認証装置は、他の装置との間で通信を行う通信手段（例えば、図１の通信部２１）と、複数の鍵を記憶する記憶手段（例えば、図１のメモリ１１）と、記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する生成手段（例えば、図１の縮退処理部１３）と、他の装置に対して、他の装置に記憶されている複数の鍵のうちの任意の数の鍵から、対応する１つの認証鍵を生成するのに必要な情報と、認証鍵を用いて暗号化するデータを通知する通知手段（例えば、図１の通信部１２）と、他の装置が認証鍵を用いて暗号化したデータを、認証鍵を用いて復号化する復号化手段（例えば、図１の暗号化部２２）とを備えることを特徴とする。

【００３２】請求項９に記載の認証装置は、他の装置との間で通信を行う通信手段（例えば、図１の通信部３３）と、複数の鍵を記憶する記憶手段（例えば、図１のメモリ３１）と、他の装置から通知された情報に基づいて、記憶手段に記憶されている複数の鍵のうちの任意の数の鍵から、１つの認証鍵を生成する生成手段（例えば、図１の縮退処理部３２）と、他の装置から通知されたデータを、認証鍵を用いて暗号化する暗号化手段（例えば、図１の暗号化部３４）とを備えることを特徴とする。

【００３３】請求項１２に記載の認証システムは、第１の装置は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、第２の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する第１の記憶手段（例えば、図９のメモリ１１）と、第１の記憶手段に記憶されている鍵と、個別データとから、認証鍵

を生成する第１の生成手段（例えば、図９の縮退処理部１３）と、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知手段（例えば、図９の制御部２４）と、第２の装置との間で通信を行う第１の通信手段（例えば、図９の通信部２１）とを備え、第２の装置は、複数の鍵と共通データを記憶する第２の記憶手段（例えば、図９のメモリ３１）と、第２の記憶手段に記憶されている複数の鍵のうち、第１の装置の通信手段からの通知に対応するものと、共通データとから、認証鍵を生成する第２の生成手段（例えば、図９の縮退処理部３２）と、第１の装置との間で通信を行う第２の通信手段（例えば、図９の通信部３３）とを備え、第１の装置と第２の装置の一方は、認証鍵を用いて暗号化を行う暗号化手段（例えば、図９の暗号化部２２）を備え、第１の装置と第２の装置の他方は、暗号化手段により暗号化されたデータを認証鍵を用いて復号化する復号化手段（例えば、図９の暗号化部３４）を備えることを特徴とする。

【００３４】請求項１３に記載の認証システムは、認証鍵は、第１の認証鍵と第２の認証鍵で構成され、第１の生成手段は、第１の記憶手段に記憶されている、自己に割り当てられている鍵と、個別データとから、第１の認証鍵を生成し、自己に割り当てられている鍵と、第１の認証鍵を用いて第２の認証鍵を生成し、第２の生成手段は、第２の記憶手段に記憶されている複数の鍵のうち、第１の装置の通知手段からの通知に対応するものと、共通データとから、第１の認証鍵を生成し、第１の認証鍵と、第２の記憶手段に記憶されている複数の鍵のうち、第１の装置の通知手段からの通知に対応するものを用いて第２の認証鍵を生成し、第１の装置と第２の装置は、いずれも暗号化手段と復号化手段を備え、第１の装置と第２の装置の一方は、乱数を生成する乱数生成手段（例えば、図９の乱数生成部２３）をさらに備え、第１の装置と第２の装置の一方の暗号化手段は、乱数生成手段で生成された乱数を第１の認証鍵を用いて暗号化し、第１の装置と第２の装置の他方の復号化手段は、第１の装置と第２の装置の一方の暗号化手段により暗号化された乱数を第１の認証鍵を用いて復号化し、第１の装置と第２の装置の他方の暗号化手段は、第１の装置と第２の装置の他方の復号化手段により復号化された乱数を、第２の認証鍵を用いて暗号化し、第１の装置と第２の装置の一方の復号化手段は、第１の装置と第２の装置の他方の暗号化手段により暗号化された乱数を第２の認証鍵を用いて復号化することを特徴とする。

【００３５】請求項１６に記載の認証システムは、第２の装置は、第１の装置の第１の通信手段から送信を受けた、第１の暗号化データと第２の暗号化データを、鍵識別番号に対応する第１の鍵を用いて復号化する第２の復号化手段（例えば、図１８の暗号化部３４）と、復号化された第２の鍵と第３の鍵が所定の関係にあるか否かを判定し、判定結果に対応して第１の鍵を第２の鍵で更新する更新手段（例えば、図１８の制御部３６）とをさらに備えることを特徴とする。

【００３６】請求項１８に記載の認証装置は、自己に割り当てられた鍵を記憶するとともに、所定の共通データと、他の装置が保持する所定の数の鍵を用いて生成された個別データを記憶する記憶手段（例えば、図９のメモリ１１）と、記憶手段に記憶されている鍵と、個別データとから、認証鍵を生成する生成手段（例えば、図９の縮退処理部１３）と、他の装置が対応する認証鍵を生成するのに必要な情報を通知する通知手段（例えば、図９の制御部２４）と、他の装置との間で通信を行う通信手段（例えば、図９の通信部２１）と、認証鍵を用いて暗号化を行う暗号化手段（例えば、図９の暗号化部２２）とを備えることを特徴とする。

【００３７】請求項２２に記載の認証装置は、複数の鍵と共通データを記憶する記憶手段（例えば、図９のメモリ３１）と、記憶手段に記憶されている複数の鍵のうち、他の装置からの通知に対応するものと、共通データとから、認証鍵を生成する生成手段（例えば、図９の縮退処理部３２）と、他の装置との間で通信を行う通信手段（例えば、図９の通信部３３）と、他の装置により暗号化されたデータを認証鍵を用いて復号化する復号化手段（例えば、図９の暗号化部３４）とを備えることを特徴とする。

【００３８】請求項２４に記載の認証装置は、他の装置から、記憶手段に記憶されている複数の鍵のうち、所定の第１の鍵を新たな第２の鍵で更新するために、第２の鍵を第１の鍵で暗号化した第１の暗号化データと、第２の鍵に対して所定の関係にある第３の鍵を、第１の鍵で暗号化した第２の暗号化データを、更新する鍵の鍵識別番号とともに送信を受けたとき、第１の暗号化データと第２の暗号化データを、更新する鍵の鍵識別番号に対応する第１の鍵を用いて復号化する第２の復号化手段（例えば、図１８の暗号化部３４）と、復号化された第２の鍵と第３の鍵が所定の関係にあるか否かを判定し、判定結果に対応して第１の鍵を第２の鍵で更新する更新手段（例えば、図１８の制御部３６）とをさらに備えることを特徴とする。

【００３９】図１は、本発明の認証システムの構成例を示している。この構成例においては、システムが、コントローラ１、リーダライタ２、およびＩＣカード３により構成されている。ＩＣカード３は、各ユーザが、例えば定期券などの代わりに所持するものであり、リーダライタには、このＩＣカード３を利用する鉄道会社の改札口に設けられているものである。なお、本明細書において、システムの用語は、複数の装置で構成されている全体の装置を総称して使用する場合に、適宜用いる。

【００４０】コントローラ１は、メモリ１１を有し、そこにＩＣカード３のメモリ３１の各エリアにアクセスす

15

るのに必要な暗号鍵と、それに対応するプロバイダ番号を記憶している。通信部１２は、リーダライタ２の通信部２１との間で有線または無線で、通信を行う。縮退処理部１３は、メモリ１１に記憶されている複数の暗号鍵の中から、所定の数の暗号鍵を読み出し、１つの縮退鍵を生成する処理を行う。制御部１４は、コントローラ１の各部の動作を制御する他、認証処理を行うようになされている。

【００４１】リーダライタ２の通信部２１は、有線または無線で、コントローラ１の通信部１２、またはＩＣカード３の通信部３３と通信を行うようになされている。暗号化部２２は、乱数生成部２３で生成した乱数を暗号化するとともに、ＩＣカード３から伝送されてきた暗号化されている乱数を復号化する処理を行う。制御部２４は、リーダライタ２の各部の動作を制御するとともに、認証処理を行うようになされている。

【００４２】ＩＣカード３は、メモリ３１を有し、このメモリ３１は、複数のエリア（図１の例の場合、５個のエリア）に区分されている。各エリアには、各プロバイダ（例えば各鉄道会社）が個別にアクセスし、適宜データを書き込み、または読み出すようになされている。ただし、各エリア毎に異なる暗号鍵が対応付けされており、所定のエリアｉにアクセスするには、対応する暗号鍵ｉが必要となる。

【００４３】縮退処理部３２は、複数の暗号鍵を縮退処理し、１つの縮退鍵を生成する処理を行う。暗号化部３４は、乱数生成部３５で生成した乱数を暗号化する処理を行うとともに、リーダライタ２より供給されてきた、暗号化されているデータを復号化する処理を行う。制御部３６は、ＩＣカード３の各部の動作を制御するとともに、認証処理を行うようになされている。

【００４４】図２は、ＩＣカード３のメモリ３１のデータ構造のより詳細な例を表している。この例においては、エリア５１は共通領域とされ、各プロバイダに共通のデータが記憶されるようになされている。また、エリア５２は、個々のプロバイダ専用の領域とされ、個々の対応するプロバイダのみが、その領域にアクセスすることができるようになされている。

【００４５】エリア５３は、エリア５１とエリア５２を管理するのに必要な情報が記録されるようになされている。その情報とは、この例の場合、個々のプロバイダに割り付けられているプロバイダ番号、そのプロバイダに対して割り付けられている領域を示すブロック割り付け情報、読み出しのみ可能、書き込みのみ可能、読み出しと書き込みの両方が可能といった許可情報、暗証鍵、および暗証鍵のバージョンとされている。

【００４６】例えば、プロバイダ番号００は、各プロバイダ共通のものとされ、そのブロック割り付け情報には、共通領域としてのエリア５１のアドレスが書き込まれている。また、その許可情報としては、共通領域としてのエリア５１に対してアクセス可能な情報が規定されている。さらに、その暗号鍵とそのバージョンとしては、共通領域としてのエリア５１に対してアクセスするのに必要な暗号鍵と、そのバージョンが規定されている。

16

【００４７】エリア５４は、システムＩＤブロックとされ、このＩＣカード３を適用するシステムのＩＤが書き込まれる。

【００４８】なお、コントローラ１のメモリ１１には、この図２に示す、プロバイダ番号、許可情報、暗号鍵バージョン、および暗号鍵が記憶されている。

【００４９】図３は、縮退処理部１３（または縮退処理部３２）の構成例を示している。ただし、この処理は、実際には、ソフトウエアにより行われる。

【００５０】すなわち、縮退処理部１３または３２においては、ＩＣカード３にｎ個の暗号鍵が存在する場合、２入力縮退回路８１－１乃至８１－（ｎ－１）の（ｎ－１）個の回路が設けられており、それぞれに２つのデータが入力され、１つのデータを出力するようになされている。２入力縮退回路８１－１には、プロバイダ１（鉄道会社１）の暗号鍵とプロバイダ２（鉄道会社２）の暗号鍵が入力されている。２入力縮退回路８１－１は、この２つの暗号鍵から１つの縮退鍵を生成し、後段の２入力縮退回路８１－２に供給する。２入力縮退回路８１－２は、２入力縮退回路８１－１より入力された縮退鍵と、プロバイダ３（鉄道会社３）の暗号鍵を縮退処理して、後段の２入力縮退回路８１－３（図示せず）に出力する。以下、同様の処理が、各２入力縮退回路８１－ｉにおいて行われ、最後の２入力縮退回路８１－（ｎ－１）で生成された縮退鍵が、最終的な１つの縮退鍵とされる。

【００５１】なお、ｎ＝１の場合（暗号鍵が１個の場合）、入力された暗号鍵が、そのまま縮退鍵として出力される。

【００５２】図４乃至図６は、図３に示した２入力縮退回路８１－ｉの構成例を表している。図４の暗号化回路８１－ｉは、前段からの入力を、予め用意されている暗号鍵に対応して暗号化し、後段に出力するようになされている。例えば、２入力縮退回路８１－１を、この暗号化回路８１－ｉで構成する場合、プロバイダ１の暗号鍵がデータとして入力され、プロバイダ２の暗号鍵が暗号鍵として入力される。そしてプロバイダ２の暗号鍵を用いて、プロバイダ１の暗号鍵（データ）を暗号化して、２入力縮退回路８１－２に出力する。

【００５３】図５の暗号化回路８１－ｉは、前段からの入力を暗号鍵として受け取り、予め用意されている暗号鍵をデータとして受け取り、暗号化処理を行って、後段に出力する。例えば、この暗号化回路８１－ｉを、図３の２入力縮退回路８１－１に応用すると、プロバイダ２の暗号鍵がデータとして入力され、プロバイダ１の暗号

鍵が暗号鍵として入力される。そして、プロバイダ２の暗号鍵をプロバイダ１の暗号鍵を利用して暗号化し、縮退鍵として、後段の２入力縮退回路８１－２に出力する。

【００５４】なお、図４と図５に示す暗号化方法としては、例えば、ＤＥＳ(Data Encryption Standard)，ＦＥＡＬ(Fast Data Encipherment Algorithm) などを用いることができる。

【００５５】図６では、暗号化回路８１－ｉが、排他的論理和回路（ＸＯＲ）により構成されている。例えば、この暗号化回路８１－ｉを、図３の２入力縮退回路８１－１に応用すると、プロバイダ１の暗号鍵とプロバイダ２の暗号鍵の排他的論理和が演算され、その演算結果が、縮退鍵として、後段の２入力縮退回路８１－２に出力されることになる。

【００５６】図３において、各プロバイダの暗号鍵は、例えば、３０バイトで表されるディジタルデータのうちの１つとされる、この場合、縮退鍵も同一のバイト数のディジタルデータとなる。暗号鍵は、３０バイトで規定される数字の中の１つであるから、すべての組み合わせの中から所定の１つの数字を選択し、順番にテストして行けば、暗号鍵を見破ることは、理論的には可能である。しかしながら、その演算を行うのには、膨大な時間がかかり、３０バイトで表される数字のどれが、実際の暗号鍵であるのかを調べるのは実質的には不可能である。

【００５７】次に、図７のタイミングチャートを参照して、その動作について説明する。なお、コントローラ１とリーダライタ２は、ここでは別の装置として示されているが、一体的な装置とすることも可能である。

【００５８】コントローラ１の制御部１４は、ステップＳ１において、通信部１２を制御し、リーダライタ２に対して充分短い周期（ＩＣカード３を所持するユーザが、鉄道駅の改札口を通過するのを検知できる周期）でポーリングを指令する。リーダライタ２の制御部２４は、通信部２１を介してこの指令を受けたとき、ステップＳ２において、通信部２１を制御し、ＩＣカード３に対するポーリングを実行する。ＩＣカード３の制御部３６は、通信部３３を介してリーダライタ２の通信部２１からポーリングの指令を受けたとき、ステップＳ３において、自己の存在を通知する。リーダライタ２の制御部２４は、通信部２１を介して、ＩＣカード３からこの通知を受けたとき、ステップＳ４において、ＩＣカード３の存在をコントローラ１に通知する。

【００５９】コントローラ１の制御部１４は、通信部１２を介してこの通知を受けたとき、ステップＳ５で縮退処理部１３を制御し、ＩＣカード３のメモリ３１のうち、アクセスすべきエリアの暗号鍵をメモリ１１から読み出させる。例えば、図１の例においては、エリア１、エリア２、およびエリア４にアクセスするため、暗号鍵

１、暗号鍵２、および暗号鍵４が、縮退処理部１３に呼び出されている。縮退処理部１３は、この３つの暗号鍵を用いて縮退処理を行う。すなわち、図３に示したように、２入力縮退回路８１－１において、暗号鍵１を暗号鍵２で暗号化し、２入力縮退回路８１－２に出力する。２入力縮退回路８１－２は、２入力縮退回路８１－１より供給された暗号鍵１と暗号鍵２を縮退した結果得られた縮退鍵を、暗号鍵３で暗号化する。そして、得られた縮退鍵が、最終的な縮退鍵とされる。

【００６０】制御部１４は、このように１つの縮退鍵が生成されると、これをプロバイダ番号（鍵の番号）とプロバイダの数（鍵の数）、および縮退処理の順序とともに、ステップＳ６において、リーダライタ２に通知させる。リーダライタ２の制御部２４は、通信部２１を介してコントローラ１の通信部１２から、この情報の入力を受けたとき、ステップＳ７において、乱数生成部２３に、乱数ｒ１を生成させる。制御部２４はこの乱数ｒ１を、ステップＳ８で通信部２１からＩＣカード３に、通知させる。このとき、制御部２４は、コントローラ１から提供を受けたプロバイダ数とプロバイダ番号も、合わせてＩＣカード３に通知する。

【００６１】ＩＣカード３の制御部３６は、このような通知を受けたとき、ステップＳ９で、まず縮退鍵生成処理を実行する。すなわち、制御部３６は、リーダライタ２から転送されてきたプロバイダ番号（鍵番号）に対応する暗号鍵をメモリ３１から読み出し、これを縮退処理部３２に供給し、縮退処理を実行させる。図１の例の場合、暗号鍵１、暗号鍵２、および暗号鍵４に対応するプロバイダ番号が転送されてくるので、縮退処理部３２は、これらのプロバイダ番号に対応する暗号鍵１、暗号鍵２、および暗号鍵４をメモリ３１から読み出し、縮退処理部３２に供給する。縮退処理部３２は、これらの３つの暗号鍵を、指定された順序（例えば、入力されたプロバイダの順序）で縮退処理し、最終的に１つの縮退鍵を生成する。これにより、コントローラ１が、ステップＳ５で生成した縮退鍵と同一の縮退鍵が、ＩＣカード３において生成されたことになる。

【００６２】次に、ステップＳ１０で、制御部３６は、リーダライタ２から通知を受けた乱数ｒ１と、縮退処理部３２で生成された縮退鍵を暗号化部３４に出力し、乱数ｒ１を縮退鍵で暗号化させる。そして、暗号化した乱数Ｒ１を生成させる。

【００６３】次に、ステップＳ１１において、制御部３６は、乱数生成部３５で、所定の乱数ｒ２を生成させる。そして、ステップＳ１２において、制御部３６は、通信部３３を制御し、ステップＳ１０で、暗号化した乱数Ｒ１と、ステップＳ１１で生成した乱数ｒ２をリーダライタ２に転送させる。

【００６４】リーダライタ２の制御部２４は、通信部２１を介して、乱数ｒ２と暗号化された乱数Ｒ１の供給を

受けたとき、ステップＳ１３で、暗号化部２２を制御し、暗号化されている乱数Ｒ１をコントローラ１より供給を受けた縮退鍵を利用して復号化させる。制御部２４は、復号化した結果得られた乱数が、ステップＳ７で生成した乱数ｒ１と等しいか否かをさらにチェックし、等しくない場合、ＩＣカード３は適正なＩＣカードではないとして、ステップＳ１４において、コントローラ１に対して、その旨を通知する。このとき、コントローラ１はエラー処理を実行する（例えば、ユーザの改札口の通過を禁止する）。

【００６５】これに対して、ステップＳ１３において、復号化された乱数と乱数ｒ１が等しいと判定された場合、ステップＳ１５に進み、制御部２４は、暗号化部２２を制御し、ＩＣカード３より供給を受けた乱数ｒ２を、コントローラ１より供給を受けた縮退鍵を用いて暗号化させ、暗号化された乱数Ｒ２を生成させる。さらに、制御部２４は、このようにして生成した、暗号化した乱数Ｒ２を、ステップＳ１６で、ＩＣカード３に転送させる。

【００６６】ＩＣカード３の制御部３６は、このように暗号化された乱数Ｒ２の供給を受けたとき、ステップＳ１７で、暗号化部３４を制御し、暗号化されている乱数Ｒ２を、ステップＳ９で生成した縮退鍵を用いて復号化させる。そして、復号化された乱数が、ステップＳ１１で生成した乱数ｒ２と等しいか否かを判定する。そして、判定した結果を、ステップＳ１８で、通信部３３を介してリーダライタ２に転送させる。

【００６７】リーダライタ２の制御部２４は、ＩＣカード３から認証結果の通知を受けたとき、ステップＳ１９で、これをさらに通信部２１からコントローラ１通知する。

【００６８】コントローラ１の制御部１４は、通信部１２を介して、この通知を受けたとき、この通知がＮＧであるとされている場合には、エラー処理を実行する。これに対してＯＫであるとされている場合（ＩＣカード３が適正なものである場合）には、ステップＳ２０において、読み出しまたは書き込みなどの必要なコマンドをリーダライタ２に出力する。リーダライタ２は、このコマンドの転送を受けたとき、ステップＳ２１で、さらにＩＣカード３に対して、読み出しまたは書き込みの指令を出力する。いまの場合、このようにして、ＩＣカード３のエリア１、エリア２、およびエリア４の読み出しまたは書き込みが指令される。

【００６９】その結果、ＩＣカード３の制御部３６は、エリア１、エリア２、またはエリア４に書き込みが指令されている場合には、書き込み処理を実行する。そして、読み出しが指令されている場合には、読み出し処理を実行する。読み出されたデータは、ステップＳ２２で、ＩＣカード３からリーダライタ２に転送され、さらに、リーダライタ２からコントローラ１に、ステップＳ２３で転送される。

【００７０】以上のように、複数のエリアにアクセスする場合に、個々に必要となる暗証鍵を個々に認証するのではなく（例えば図１の例の場合、暗号鍵１、暗号鍵２、暗号鍵４について、個々に認証処理を行う（すなわち、合計３回の認証処理を行う）のではなく）、複数の暗証鍵から１つの縮退鍵を生成し、この１つの縮退鍵で１回だけ認証処理を行うようにしたので、迅速な認証処理が可能となる。

【００７１】なお、縮退鍵は、暗号鍵と同一のバイト数（長さ）としたが、異なるバイト数とすることも可能である。ただし、この縮退鍵は、認証に用いるだけなので、その縮退鍵から元の複数の暗号鍵を復元することが可能である必要はない。

【００７２】図８は、縮退鍵を生成する他の方法を表している。この例においては、プロバイダ１乃至プロバイダｎそれぞれに、暗号鍵Ｋ１乃至Ｋｎが割り当てられる他、最初の２入力縮退回路８１－１に、予め含められた秘密（各プロバイダに共通のデータとされるので、必ずしも秘密でなくともよいが）のデータＤ０が入力され、２入力縮退回路８１－１は、このデータＤ０を、プロバイダ１の暗号鍵Ｋ１に基づいて暗号化するようになされている。そして、２入力縮退回路８１－２が、２入力縮退回路８１－１の出力Ｄ１を、プロバイダ２の暗号鍵Ｋ２に基づいて暗号化するようになされている。以下、順次、同様の処理が、２入力縮退回路８１－ｉにおいて行われ、最終段の２入力縮退回路８１－ｎの出力が最終的な縮退鍵とされる。

【００７３】図３に示すように縮退鍵を生成する場合、プロバイダ２は、プロバイダ１の暗号鍵を知らないと、縮退鍵を生成することができない。基本的に、各プロバイダは独立しているので、所定のプロバイダの暗号鍵を他のプロバイダに知らせるようにすることは、秘密性を確保する上で好ましいことではない。

【００７４】これに対して、図８に示すように縮退鍵を生成すると、自分自身の暗号鍵を他のプロバイダに通知しなくても、他のプロバイダは、縮退鍵を生成することができる。

【００７５】図９乃至図１１は、図８に示すように、縮退鍵を生成する場合のプロバイダ１、プロバイダ２、またはプロバイダ４の、コントローラ１およびリーダライタ２と、ＩＣカード３の構成例を表している。

【００７６】これらの図に示すように、ＩＣカード３には、メモリ３１に、エリア１乃至エリア５に対応する暗号鍵Ｋ１乃至暗号鍵Ｋ５の他、所定のデータ（共通データ）Ｄ０が予め記憶されている。

【００７７】そして、プロバイダ１のメモリ１１には、自分自身の暗号鍵Ｋ１とデータＤ０２４が記憶されており（図９）、プロバイダ２のメモリ１１には、自分自身の暗号鍵Ｋ２とデータＤ０１４が記憶されており（図１

０）、プロバイダ４のメモリ１１には、自分自身の暗号鍵Ｋ４とデータＤ０１２が記憶されている（図１１）。

【００７８】これらのデータ（個別データ）Ｄ０２４，Ｄ０１４，Ｄ０１２は、図１２乃至図１４に示す方法で生成されたものである。

【００７９】すなわち、プロバイダ１は、データＤ０２４を得るために、予め定めたデータＤ０を、プロバイダ２により、その暗号鍵Ｋ２を用いて、２入力縮退回路８１－１で縮退して、データＤ０２を生成してもらう。そして、このデータＤ０２をプロバイダ４に提供して、その暗号鍵Ｋ４で２入力縮退回路８１－２で縮退して、データＤ０２４を生成してもらう。プロバイダ１は、このデータＤ０２４をプロバイダ４から提供を受け、メモリ１１に記憶させる。

【００８０】なお、この場合、データＤ０を先にプロバイダ４に提供し、暗号鍵Ｋ４で縮退して、データＤ０４を生成してもらい、このデータＤ０４をプロバイダ２に提供して、暗号鍵Ｋ２で縮退して、データＤ０４２を生成してもらい、これをメモリ１１に記憶させるようにしてもよい。そこで、プロバイダ１は、いずれの順序で縮退を行ったのかを示す縮退の順番もメモリ１１に記憶しておく。

【００８１】また、図１３に示すように、プロバイダ２は、プロバイダ１に依頼して、その暗号鍵Ｋ１でデータＤ０を縮退したデータＤ０１を生成してもらう。そして、このデータＤ０１をプロバイダ４に提供して、暗号鍵Ｋ４で縮退してもらい、データＤ０１４を生成してもらう。そして、このデータＤ０１４をメモリ１１に記憶させる。なお、この場合も、先にプロバイダ４に縮退処理を依頼して、暗号鍵Ｋ４を用いて生成されたデータＤ０４をプロバイダ１に提供し、これをさらに暗号鍵Ｋ１を用いて縮退してもらい、データＤ０４１を得て、これをメモリ１１に記憶させるようにしてもよい。プロバイダ２は、縮退の順番もメモリ１１に記憶させる。

【００８２】さらに、図１４に示すように、プロバイダ４は、プロバイダ１に依頼して、データＤ０を暗号鍵Ｋ１を用いて縮退し、データＤ０１を生成してもらう。そして、このデータＤ０１をプロバイダ２に提供して、暗号鍵Ｋ２を用いて縮退し、データＤ０１２を生成してもらう。このデータＤ０１２をメモリ１１に記憶させる。この場合も同様に、先にプロバイダ２にデータＤ０を暗号鍵Ｋ２を用いて縮退し、データＤ０２を生成し、このデータＤ０２をプロバイダ１により暗号鍵Ｋ１を用いて縮退し、データＤ０２１を生成してもらうようにしてもよい。プロバイダ４も、縮退の順序をメモリ１１に記憶させておく。

【００８３】各プロバイダは、次のように認証処理を行うことができる。例えば、プロバイダ１においては、図９に示すように、制御部１４が縮退処理部１３を制御し、メモリ１１からデータＤ０２４と暗号鍵Ｋ１を読み出し、縮退鍵を生成させる。この縮退鍵は、リーダライタ２に転送される。このとき、リーダライタ２には、プロバイダの数（この例の場合、３）、プロバイダ番号（いまの場合、プロバイダ１、プロバイダ２、およびプロバイダ４）、並びに、縮退の順序（いまの場合、プロバイダ２、プロバイダ４、プロバイダ１の順）を通知する。制御部２４は、通信部２１を制御し、コントローラ１の制御部１４から転送されてきたこれらのプロバイダ数、プロバイダ番号、および縮退順序の情報を、ＩＣカード３に通知する。

【００８４】ＩＣカード３においては、通信部３３でこれらの情報を受信すると、制御部３６は、これらの情報に対応して縮退処理部３２を制御し、縮退鍵を生成させる。縮退処理部３２は、メモリ３１からデータＤ０を読み出し、これを指定された順序と指定されたプロバイダの番号の暗号鍵を用いて、順次縮退する。すなわち、データＤ０を暗号鍵Ｋ２を用いて縮退し、データＤ０２を得る。このデータＤ０２を暗号鍵Ｋ４を用いて縮退し、データＤ０２４を得る。さらに、このデータＤ０２４を暗号鍵Ｋ１を用いて、縮退鍵を生成する。このようにして生成された縮退鍵は、コントローラ１の縮退処理部１３が生成した縮退鍵と同一の縮退鍵となっている。

【００８５】従って、以下、図７を参照して説明した場合と同様に、ステップＳ１０以降の処理を行って、認証処理を行うことができる。そして、プロバイダ１のリーダライタ２は、ＩＣカード３のメモリ３１のエリア１、エリア２、およびエリア４にアクセスすることが可能となる。

【００８６】一方、プロバイダ２においては、図１０に示すように、制御部１４は、縮退処理部１３を制御し、メモリ１１からデータＤ０１４を読み出し、これを、やはりメモリ１１から読み出した暗号鍵Ｋ２を用いて縮退させる。そして、生成した縮退鍵をリーダライタ２に転送する。このとき、リーダライタ２には、プロバイダ数（いまの場合、３）、プロバイダ番号（いまの場合、プロバイダ１、プロバイダ２、およびプロバイダ４）、および縮退処理の順番（いまの場合、プロバイダ１、プロバイダ４、プロバイダ２の順番）が、リーダライタ２に通知される。

【００８７】リーダライタ２は、これらの情報をＩＣカード３に転送する。ＩＣカード３においては、これらの情報に対応して、縮退鍵が生成される。

【００８８】すなわち、ＩＣカード３の縮退処理部３２は、メモリ３１から、データＤ０を読み出し、これを最初に暗号鍵Ｋ１を用いて縮退し、データＤ０１を得る。そして、このデータＤ０１がさらに暗号鍵Ｋ４を用いて縮退され、データＤ０１４が生成される。このデータＤ０１４は、さらに暗号鍵Ｋ２を用いて縮退される。このようにして生成された縮退鍵は、コントローラ１において生成された縮退鍵と同一の縮退鍵となっている。従っ

て、プロバイダ２のリーダライタ２は、ＩＣカード３のメモリ３１のエリア１、エリア２、およびエリア４に対してアクセスすることができる。

【００８９】さらに、図１１に示すように、プロバイダ４においても、コントローラ１の制御部１４が縮退処理部１３を制御し、メモリ１１に記憶されているデータＤ０１２を暗号鍵Ｋ４を用いて縮退鍵を生成し、これをリーダライタ２に転送する。このとき、プロバイダ数（いまの場合、３）、プロバイダ番号（いまの場合、プロバイダ１、プロバイダ２、およびプロバイダ４）、および縮退順序（いまの場合、プロバイダ１、プロバイダ２、プロバイダ４の順番）が通知される。これらの情報は、ＩＣカード３に転送される。ＩＣカード３は、これらの情報に基づいて、縮退処理を実行する。

【００９０】すなわち；縮退処理部３２は、メモリ３１からデータＤ０を読み出し、これを暗号鍵Ｋ１を用いてデータＤ０１を生成する。次に、このデータＤ０１を暗号鍵Ｋ２を用いて縮退し、データＤ０１２を生成する。そして、このデータＤ０１２が、さらに暗号鍵Ｋ４を用いて縮退され、最終的な縮退鍵が生成される。このようにして生成された縮退鍵は、コントローラ１において生成された縮退鍵と同一となっている。従って、リーダライタ２は、ＩＣカード３のメモリ３１のエリア１、エリア２、およびエリア４に対してアクセスすることができる。

【００９１】図１５は、さらに他の縮退鍵生成の方法を表している。この方法においては、最終的な縮退鍵を生成する２入力縮退回路８１－ｎに入力されるデータＤｎ－１と、ＩＣカード３が予め保持しているＩＤ番号とを演算して、その演算結果に対して暗号鍵Ｋｎを用いて縮退鍵を生成するようにしている。その他の処理は、図８における場合と同様である。

【００９２】図１６は、図１５に示す方法に従って、縮退鍵を生成する場合のコントローラ１、リーダライタ２、およびＩＣカード３の構成例を表している。なお、この構成は、プロバイダ４の構成を表している。同図に示すように、コントローラ１のメモリ１１は、データＤ０１２と暗号鍵Ｋ４、並びに縮退順序を記憶している。リーダライタ２は、通信部２１が受信したデータからＩＤを取得するＩＤ取得部２１１を有している。また、ＩＣカード３は、メモリ２０１（メモリ３１と同一のメモリとすることもできる）に、ＩＣカード３に固有のＩＤ番号が予め記憶されている。

【００９３】このように、ＩＤ番号を用いて認証処理を行うようにすると、同一のプロバイダの組み合わせ（例えばプロバイダ１、プロバイダ２、およびプロバイダ４の組み合わせ）のＩＣカードを所持している複数のユーザが、近接した状態で、所定のプロバイダの改札口を通過するような場合の混乱を避けることができる。

【００９４】すなわち、複数のＩＣカード３が所定のプロバイダのリーダライタ２の近傍を通過するとき、リーダライタ２からの要求に対して、複数のＩＣカード３がそれぞれ応答することになり、リーダライタ２がいずれのＩＣカードからの応答であるのかを判別することができず、誤った処理が行われるおそれがある。これに対して、ＩＤ番号を用いると、このような混乱を避けることができる。

【００９５】例えば、図１７に示すように、ＩＣカード３ＡとＩＣカード３Ｂが、リーダライタ２の近傍を通過しようとすると、リーダライタ２が、ステップＳ４１において、ＩＣカード３に対してＩＤを要求する。この要求は、ＩＣカード３Ａの通信部３３だけでなく、ＩＣカード３Ｂの通信部３３でも受信される。ＩＣカード３Ａの制御部３６は、このようにしてＩＤ要求信号を受信すると、ステップＳ４２において、乱数生成部３５を制御し、所定の乱数を発生させる。そして、ステップＳ４３において、発生された乱数に対応するタイムスロットの割当処理を実行する。すなわち、リーダライタ２とＩＣカード３の間の通信は、時分割多重動作で行われ、ＩＣカード３Ａは、その複数のタイムスロットのうち、発生された乱数に対応するタイムスロットを、自己の通信のタイムスロットとして割り当てる。そして、割り当てたタイムスロットのタイミングにおいて、ＩＣカード３Ａの制御部３６がメモリ２０１から読み出したＩＤ番号（ID_A）を、通信部３３を介して、ステップＳ４４でリーダライタ２に送信させる。

【００９６】同様の処理が、他のＩＣカード３Ｂにおいても実行される。すなわち、ＩＣカード３Ｂの制御部３６は、リーダライタ２からＩＤ要求信号を受信すると、ステップＳ４５で乱数生成部３５を制御し、乱数を発生させる。そして、ステップＳ４６において、生成された乱数に対応するタイムスロットを、自己のタイムスロットとして割り当てる。ステップＳ４７において、メモリ２０１に記憶されているＩＤ番号（ID_B）を読み出し、割り当てられたタイムスロットのタイミングで、リーダライタ２に転送する。

【００９７】リーダライタ２においては、ＩＣカード３Ａ，３Ｂから送信されてきたＩＤ番号を通信部２１で受信すると、これをＩＤ取得部２１１に供給し、記憶させる。そして、ステップＳ４８において、制御部２４は、乱数生成部２３を制御し、乱数ｒ１を生成させる。さらに、ステップＳ４９において、制御部２４は、取得したＩＤのうち、例えば先に取得した方を選択する。制御部２４は、さらに、コントローラ１のメモリ１１から、データＤ０１２、暗号鍵Ｋ４、および縮退順序の情報の提供を受ける。そして、これらの情報に対応して、縮退鍵を生成する。

【００９８】最初に、制御部２４は、データＤ０１２に、この選択したＩＤ（例えば、ＩＣカード３のID_A）に対して、所定の演算を施す。この演算は、加

25

算、排他的論理和の演算などとすることができる。制御部２４は、この演算結果を暗号鍵Ｋ４を用いて縮退し、縮退鍵を生成する。

【００９９】さらに、ステップＳ５０において、プロバイダ数、プロバイダ番号、縮退順序、および乱数ｒ１が、ＩＣカード３に送信される。この情報は、ＩＣカード３Ａと、ＩＣカード３Ｂの両方において受信される。ＩＣカード３Ｂは、この情報を受信したとき、ステップＳ５１で、指定された順序に従って、データＤ０を暗号鍵Ｋ１で縮退し、データＤ０１を得、これを暗号鍵Ｋ２で縮退して、データＤ０１２を得る。そして、さらに、メモリ２０１からＩＤ$_4$を読み取り、データＤ０１２と演算した結果を、暗号鍵Ｋ４で縮退する。

【０１００】このようにして生成した縮退鍵を用いて、暗号化部３４が、暗号化されている乱数ｒ１を復号化する。しかしながら、この乱数ｒ１は、ＩＤ$_4$を用いて生成した縮退鍵で暗号化されているため、ＩＤ$_4$を用いて生成した縮退鍵では復号化することができない。従って、ＩＣカード３Ｂは、以後、リーダライタ２からの送信に対して応答しない。

【０１０１】これに対して、ＩＣカード３Ａにおいては、ステップＳ５２で、制御部３６が、リーダライタ２から転送されてきた情報に対応して、縮退鍵を生成する。すなわち、指定された縮退順序に従って、ＩＣカード３Ａの縮退処理部３２は、最初にメモリ３１から読み出したデータＤ０を、エリア１から読み出した暗号鍵Ｋ１を用いて縮退し、データＤ０１を生成する。そして、このデータＤ０１をエリア２から読み出した暗号鍵Ｋ２を用いて縮退し、データＤ０１２を生成する。さらに、このデータＤ０１２とメモリ２０１から読み出したＩＤ番号（ＩＤ$_4$）とに対して所定の演算を施し、その演算結果に対して、メモリ３１のエリア４から読み出した暗号鍵Ｋ４を用いて縮退処理を行い、縮退鍵を生成する。このようにして生成した縮退鍵は、リーダライタ２がステップＳ４９で生成した縮退鍵と同一の縮退鍵となる。

【０１０２】従って、以後、ステップＳ５３乃至ステップＳ５９に示す、図７におけるステップＳ１０乃至ステップＳ１７に対応する処理を実行して、認証処理を行うことができる。その処理は、図７において説明した場合と同様であるので、その説明は省略する。

【０１０３】図１８は、暗号鍵を変更する方法を表している。例えば、プロバイダ１がその暗号鍵Ｋ１を変更しようとする場合、所定の乱数ｅ１を発生し、これを新たな鍵Ｋ１’とする。このように、自分自身の暗号鍵を変更したとき、プロバイダ１は、自分自身のリーダライタ２を利用するユーザのＩＣカード３のメモリ３１に記憶されているエリア１の暗号鍵Ｋ１は、適宜自分でこれを更新することができる。しかしながら、他のプロバイダ２、またはプロバイダ４のリーダライタ２を使用するユーザのＩＣカード３の暗号鍵Ｋ１も更新する必要がある。この場合、プロバイダ１は、他のプロバイダ２またはプロバイダ４に対して、新たな暗号鍵Ｋ１’を教えずに、暗号鍵Ｋ１を新たな暗号鍵Ｋ１’に更新させることができる。

26

【０１０４】この場合、プロバイダ１は、最初に次式を演算して、データＣ１，Ｃ２を生成する。

Ｃ１＝Ｅ（ｅ１，Ｋ１）

Ｃ２＝Ｅ（ｅ２，Ｋ１）

【０１０５】なお、ここで、Ｅ（Ａ，Ｂ）は、データＡを鍵Ｂを用いて暗号化することを意味する。暗号化の方法としては、ＤＥＳ，ＦＥＡＬなどを用いることができる。

【０１０６】また、ｅ２は、次式を満足する値である。

ｅ１＋ｅ２＝Ｆ

【０１０７】なお、この値Ｆは、予め定められている値であり、他のプロバイダ２、プロバイダ４も、自分自身の暗号鍵を変更する場合に用いるものとして知っている値であり、ＩＣカード３にも、メモリ３１に予め記憶されている。

【０１０８】プロバイダ１は、このようにして、データＣ１，Ｃ２を生成すると、この値を、自分自身の暗号鍵Ｋ１に割り当てられている鍵番号（いまの場合、鍵番号１）とともに、他のプロバイダに通知する。各プロバイダは、これらのデータを用いて、そのリーダライタ２を使用するＩＣカード３のメモリ３１内の鍵Ｋ１を、次のようにして更新する。この更新処理について、プロバイダ４を例として次に説明する。

【０１０９】すなわち、プロバイダ４のリーダライタ２は、ＩＣカード３に対して、データＣ１，Ｃ２を送信する。ＩＣカード３の暗号化部３４は、次式を演算して、ｅ１，ｅ２を求める。

ｅ１＝Ｄ（Ｃ１，Ｋ１）

ｅ２＝Ｄ（Ｃ２，Ｋ１）

【０１１０】なお、ここで、Ｄ（Ａ，Ｂ）は、データＡを鍵Ｂを用いて復号化することを意味する。

【０１１１】すなわち、ＩＣカード３は、メモリ３１に記憶されている鍵Ｋ１を用いて、データＣ１，Ｃ２を復号化し、データｅ１，ｅ２を得ることができる。

【０１１２】制御部３６は、さらに、以上のようにして得たｅ１とｅ２を加算し、その加算結果がメモリ３１に予め記憶されている所定の値Ｆと等しいか否かを判定する。等しい場合には、データＣ１を復号して得られるデータｅ１を、鍵Ｋ１に代わる新たな鍵Ｋ１’として更新する。

【０１１３】これに対して、ｅ１とｅ２の和がＦと異なる場合、不正な更新の要求であるとして、更新処理を行わないようにする。

【０１１４】例えば、悪意を持ったプロバイダが、プロバイダ１の暗号鍵Ｋ１を改ざんしようとして、次式を演算して、ｅ１’，ｅ２’を得たとする。

ｅ１’＝Ｄ（Ｃ１’，Ｋ１）

ｅ２’＝Ｄ（Ｃ２’，Ｋ１）

【０１１５】このＣ１’，Ｃ２’は、改ざんを試みたプロバイダが適当に設定した値である。

【０１１６】しかしながら、このようにして生成されたｅ１’とｅ２’を加算しても、その加算結果は、一般的には、値Ｆには等しくならない。この値Ｆになるｅ１’，ｅ２’の組み合わせを発見するには、相当の時間を必要とし、実質的には極めて困難である。従って、第３者が、他人の暗号鍵を改ざんすることが防止される。

【０１１７】なお、プロバイダ２も同様の処理を行って、そのリーダライタ２を利用するＩＣカード３のメモリ３１の暗号鍵Ｋ１を更新する。

【０１１８】なお、以上のようにして、プロバイダ１の暗号鍵Ｋ１が変更された場合、プロバイダ１、プロバイダ２、およびプロバイダ４は、図１２乃至図１４を参照して説明した場合と同様の処理を再び行い、それぞれに記憶するデータＤ０２４，Ｄ０１４，Ｄ０１２を更新する。

【０１１９】図１９は、認証処理のさらに他の方法を示している。なお、この図１９のリーダライタ２は、プロバイダ４のリーダライタを表している。

【０１２０】この例においては、制御部２４が、メモリ１１に記憶されている暗号鍵Ｋ４とデータＤ０１２を用いて、縮退鍵Ｋｓを生成する。そして、制御部２４は、例えば、暗号鍵Ｋ４の偶数ビットと縮退鍵Ｋｓの奇数ビットとを合成し、第１の縮退鍵$K_{,,1}$を生成し、暗号鍵Ｋ４の奇数ビットと縮退鍵Ｋｓの偶数ビットとを合成し、第２の縮退鍵$K_{,,2}$を生成する。

【０１２１】第１の縮退鍵$K_{,,1}$は、暗号化部２２の暗号化部２２Ａに入力され、乱数生成部２３で生成された乱数を暗号化するのに用いられる。この暗号化された乱数は、ＩＣカード３に送信される。また、このとき、上述した場合と同様にして、縮退鍵を生成するのに必要な情報が、同時にＩＣカード３に送信される。

【０１２２】ＩＣカード３は、この情報を用いて、メモリ３１からデータＤ０を読み出し、さらに暗号鍵Ｋ１，Ｋ２，Ｋ４を順次適用して、縮退鍵Ｋｓを生成する。この縮退鍵Ｋｓは、リーダライタ２が生成した縮退鍵Ｋｓと同一の値となっている。

【０１２３】制御部３６は、リーダライタ２と同様の処理を行うことで、第１の縮退鍵$K_{,,1}$と第２の縮退鍵$K_{,,2}$を生成する。

【０１２４】そして、暗号化部３４の復号化部３４Ｂは、リーダライタ２より送信されてきた暗号化されている乱数を復号化し、この復号化した乱数を暗号化部３４Ａに転送する。暗号化部３４Ａにおいては、第２の縮退鍵$K_{,,2}$を用いて暗号化し、リーダライタ２に送信する。

【０１２５】リーダライタ２においては、暗号化部２２

の復号化部２２Ｂで、ＩＣカード３より送信されてきた暗号化されている乱数を、第２の縮退鍵$K_{,,2}$を用いて復号化する。復号結果は、制御部２４に転送される。

【０１２６】このようにして復号された乱数は、ＩＣカード３が適正なものであれば、乱数生成部２３で生成した乱数と同一の乱数となっている。従って、この受信した乱数が生成した乱数と等しいか否かを調べることで、認証処理を行うことができる。

【０１２７】

【発明の効果】以上の如く、請求項１に記載の認証システムおよび請求項５に記載の認証方法によれば、複数の鍵から１つの認証鍵を生成し、この認証鍵を用いて、暗号化と復号化を行うようにしたので、より迅速な認証を行うことが可能なシステムを実現することができる。

【０１２８】請求項６に記載の認証装置および請求項８に記載の認証方法によれば、他の装置に対して認証鍵を生成するのに必要な情報を通知し、他の装置が、その情報に基づいて生成した認証鍵を用いて、暗号化したデータを復号化するようにしたので、他の装置との間において、迅速な認証処理が可能となる。

【０１２９】請求項９に記載の認証装置および請求項１１に記載の認証方法によれば、他の装置から通知された情報に基づいて、１つの認証鍵を生成し、やはり他の装置から通知されたデータを、その認証鍵を用いて、暗号化するようにしたので、他の装置との間で、迅速な認証処理が可能となる装置を提供することが可能となる。

【０１３０】請求項１２に記載の認証システムおよび請求項１７に記載の認証方法によれば、第１の装置で、自己に割り当てられた鍵と、個別データとから、認証鍵を生成し、第２の装置で、第１の装置からの通知と、共通データとから、認証鍵を生成するようにしたので、より秘密性を保持しつつ、他の装置との間において、迅速な認証処理が可能となる。

【０１３１】請求項１８に記載の認証装置および請求項２１に記載の認証方法によれば、自己に割り当てられた鍵と、個別データとから、認証鍵を生成するようにしたので、秘密性を確保しつつ、他の装置との間において、迅速な認証処理が可能となる。

【０１３２】請求項２２に記載の認証装置および請求項２５に記載の認証方法によれば、他の装置からの通知に対応する鍵と、共通データとから、認証鍵を生成するようにしたので、秘密性を確保しつつ、他の装置との間において、迅速な認証処理が可能となる。

【図面の簡単な説明】

【図１】本発明の認証システムの構成例を示すブロック図である。

【図２】図１のメモリ３１のデータ構造の例を示す図である。

【図３】図１の縮退処理部１３の構成例を示す図である。

29

【図４】図３の２入力縮退回路の構成例を示す図である。

【図５】図３の２入力縮退回路の構成例を示す図である。

【図６】図３の２入力縮退回路の構成例を示す図である。

【図７】図１の認証システムの動作を説明するタイミングチャートである。

【図８】図１の縮退処理部１３の他の構成例を示す図である。

【図９】図８に示す構成例で縮退鍵を生成する場合におけるプロバイダ１の認証システムの構成例を示すブロック図である。

【図１０】図８に示す構成例で縮退鍵を生成する場合におけるプロバイダ２の認証システムの構成例を示すブロック図である。

【図１１】図８に示す構成例で縮退鍵を生成する場合におけるプロバイダ４の認証システムの構成例を示すブロック図である。

【図１２】図９のメモリ１１に記憶するデータの生成を説明する図である。

【図１３】図１０のメモリ１１に記憶するデータの生成

30

を説明する図である。

【図１４】図１１のメモリ１１に記憶するデータの生成を説明する図である。

【図１５】図１の縮退処理部１３のさらに他の構成例を示す図である。

【図１６】図１５に示す方法で縮退鍵を生成する場合のプロバイダ４の認証システムの構成例を示すブロック図である。

【図１７】図１６の例の動作を説明するタイミングチャートである。

【図１８】鍵を変更する場合の動作を説明する図である。

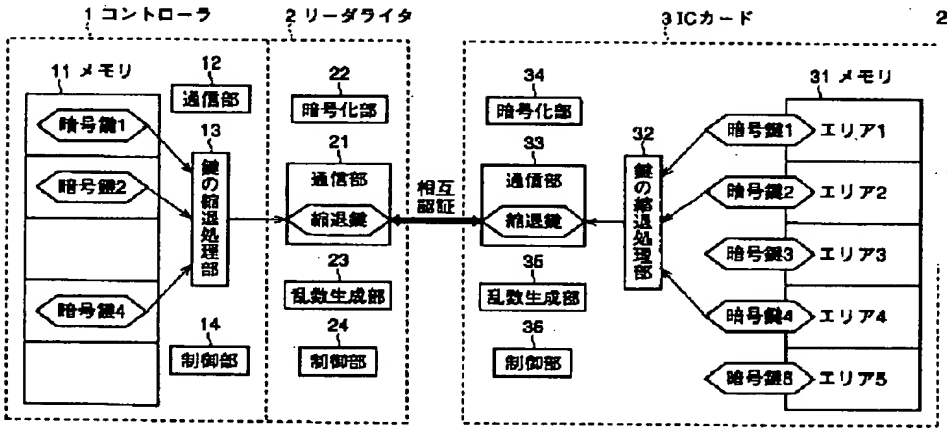
【図１９】他の認証処理を説明するブロック図である。

【図２０】従来の認証システムの構成を示す図である。

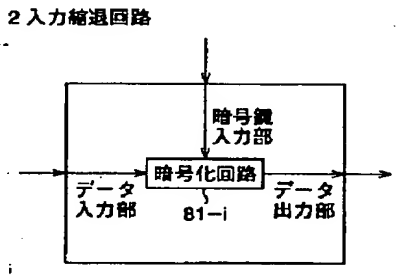
【符号の説明】

１　コントローラ，　２　リーダライタ，　３　ＩＣカード，　１１　メモリ，　１２　通信部，　１３　縮退処理部，　１４　制御部，　２１　通信部，２２　暗号化部，　２３　乱数生成部，　２４　制御部，　３１　メモリ，　３２　縮退処理部，　３３　通信部，　３４　暗号化部，　３５　乱数生成部，３６　制御部

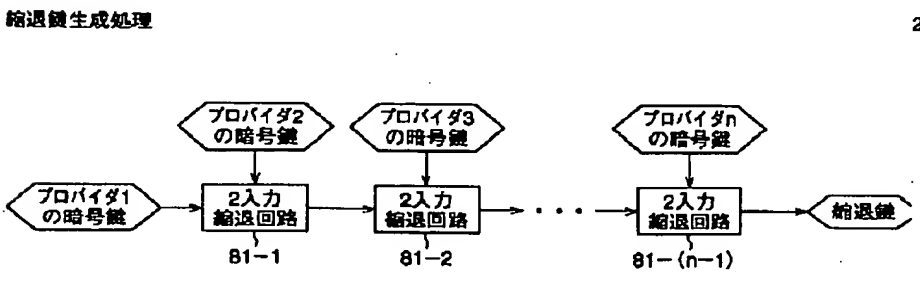
【図１】



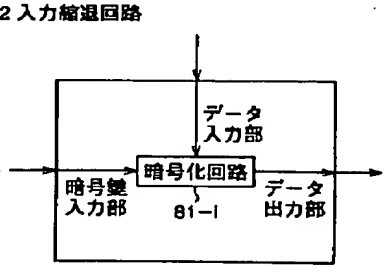
【図４】



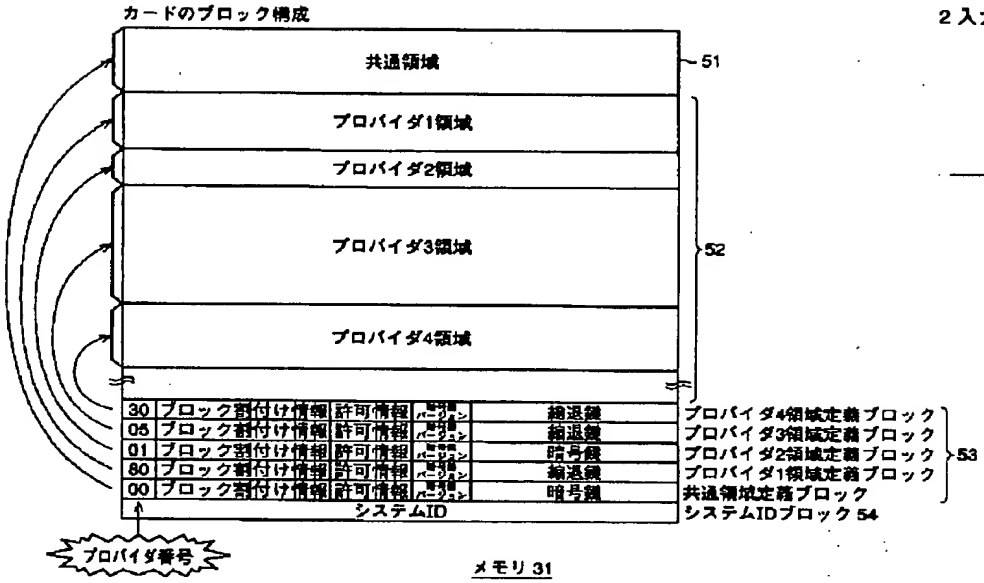
【図３】



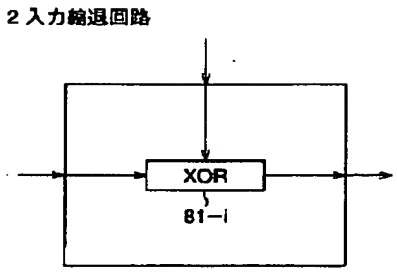
【図５】



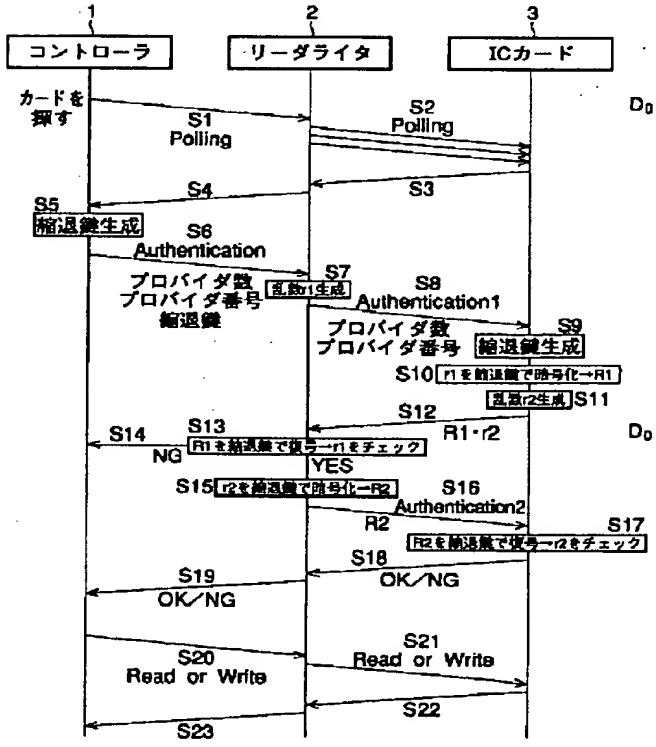
【図２】



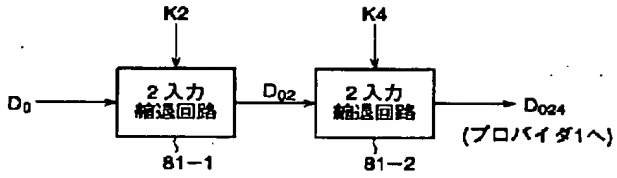
【図６】



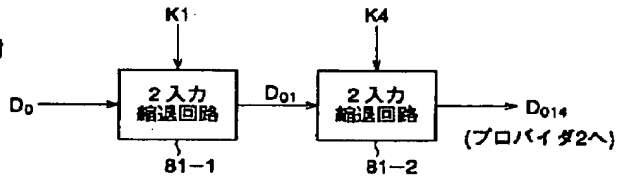
【図７】



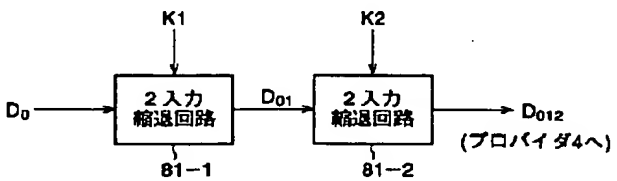
【図１２】



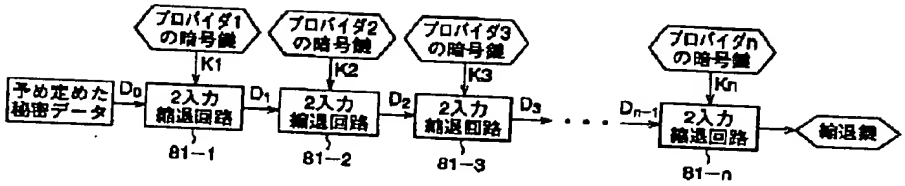
【図１３】



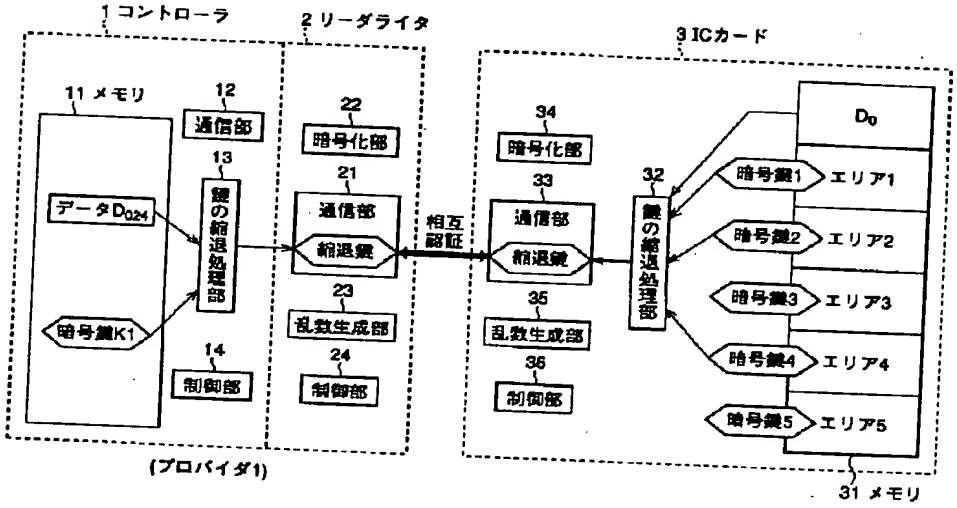
【図１４】



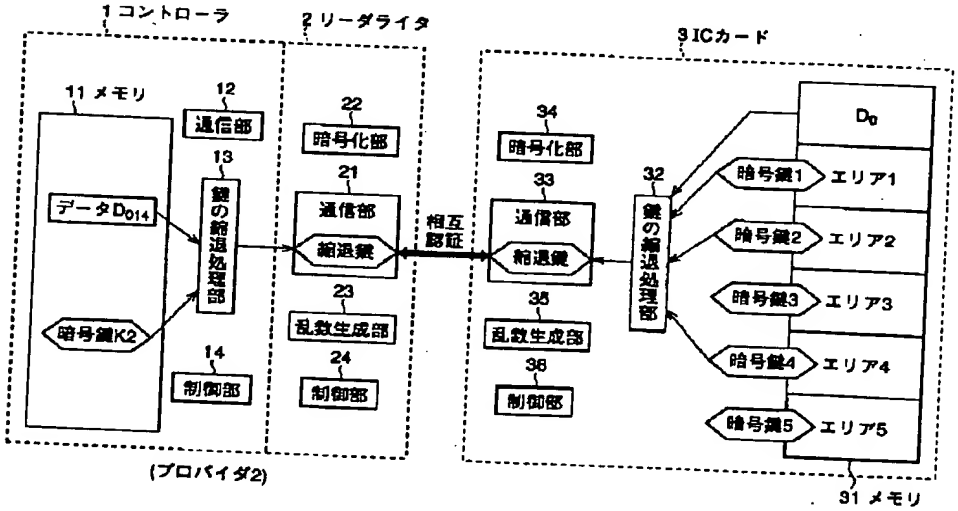
【図８】


プロバイダ1の暗号鍵
K1
プロバイダ2の暗号鍵
K2
プロバイダ3の暗号鍵
K3
プロバイダnの暗号鍵
Kn
予め定めた秘密データ
D0
2入力縮退回路
D1
D2
D3
Dn-1
81−1
81−2
81−3
81−n
縮退鍵

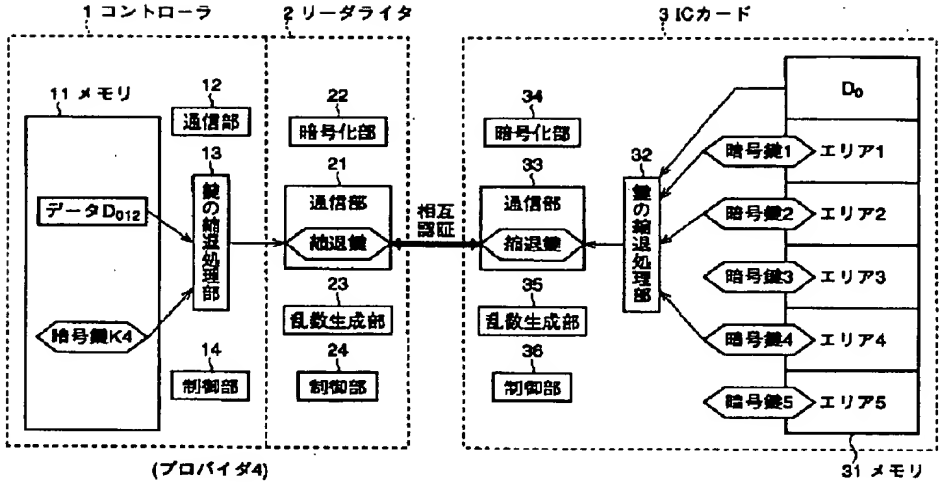
【図９】


1 コントローラ
2 リーダライタ
3 ICカード
11 メモリ
12 通信部
13 鍵の縮退処理部
14 制御部
22 暗号化部
21 通信部
縮退鍵
23 乱数生成部
24 制御部
相互認証
34 暗号化部
33 通信部
縮退鍵
35 乱数生成部
36 制御部
32 鍵の縮退処理部
D0
暗号鍵1 エリア1
暗号鍵2 エリア2
暗号鍵3 エリア3
暗号鍵4 エリア4
暗号鍵5 エリア5
データ D024
暗号鍵K1
(プロバイダ1)
31 メモリ

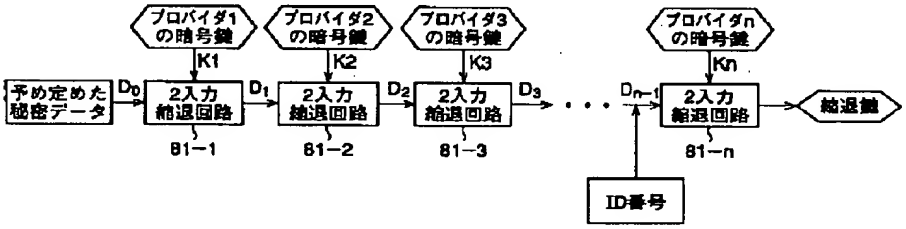
【図１０】


1 コントローラ
2 リーダライタ
3 ICカード
11 メモリ
12 通信部
13 鍵の縮退処理部
14 制御部
22 暗号化部
21 通信部
縮退鍵
23 乱数生成部
24 制御部
相互認証
34 暗号化部
33 通信部
縮退鍵
35 乱数生成部
36 制御部
32 鍵の縮退処理部
D0
暗号鍵1 エリア1
暗号鍵2 エリア2
暗号鍵3 エリア3
暗号鍵4 エリア4
暗号鍵5 エリア5
データ D014
暗号鍵K2
(プロバイダ2)
31 メモリ

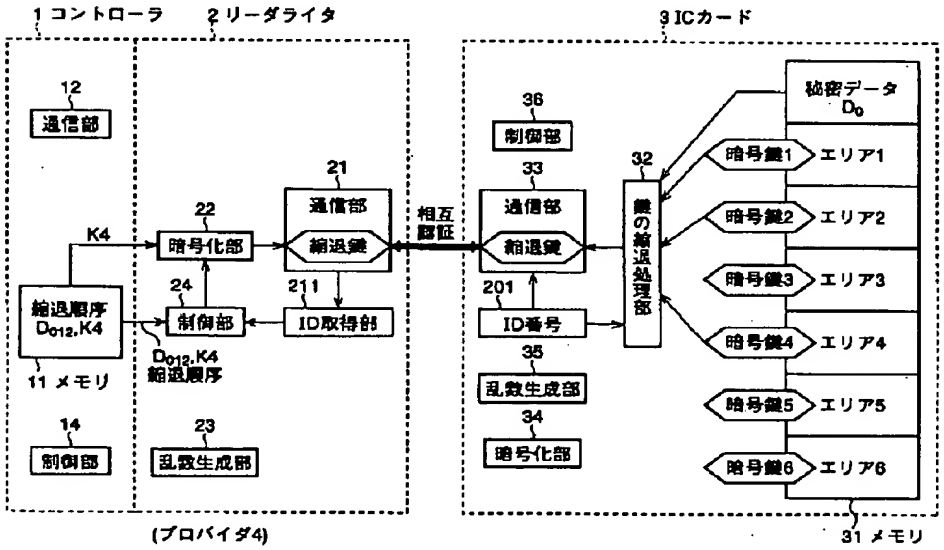
【図１１】


1 コントローラ
2 リーダライタ
3 ICカード
11 メモリ
12
通信部
13
鍵の縮退処理部
14
制御部
データD_{012}
暗号鍵K4
22
暗号化部
21
通信部
縮退鍵
23
乱数生成部
24
制御部
相互認証
34
暗号化部
33
通信部
縮退鍵
35
乱数生成部
36
制御部
32
鍵の縮退処理部
D_0
暗号鍵1
エリア1
暗号鍵2
エリア2
暗号鍵3
エリア3
暗号鍵4
エリア4
暗号鍵5
エリア5
(プロバイダ4)
31 メモリ

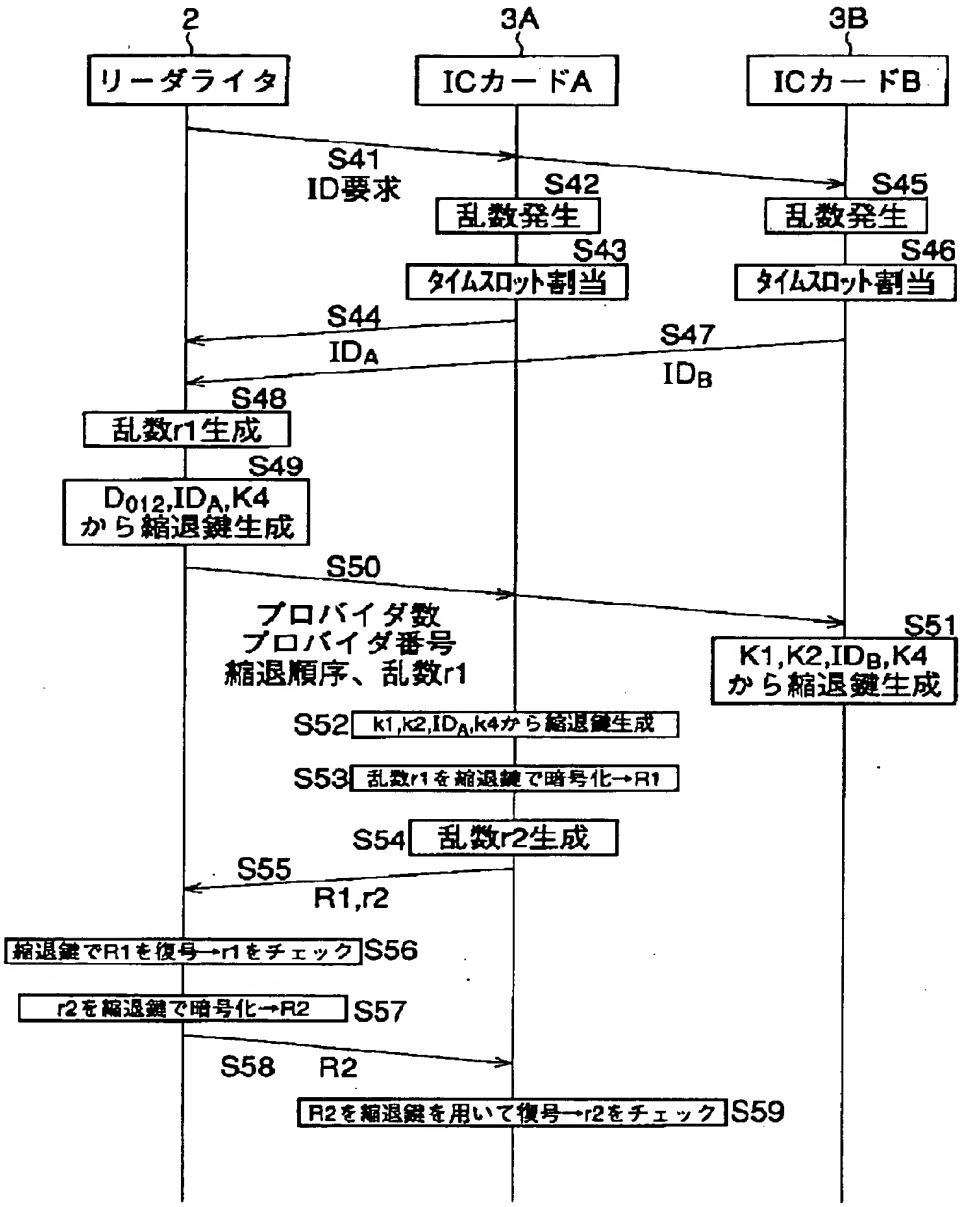
【図１５】


プロバイダ1の暗号鍵
プロバイダ2の暗号鍵
プロバイダ3の暗号鍵
プロバイダnの暗号鍵
K1
K2
K3
Kn
予め定めた秘密データ
D_0
2入力縮退回路
D_1
D_2
D_3
D_{n-1}
縮退鍵
81−1
81−2
81−3
81−n
ID番号

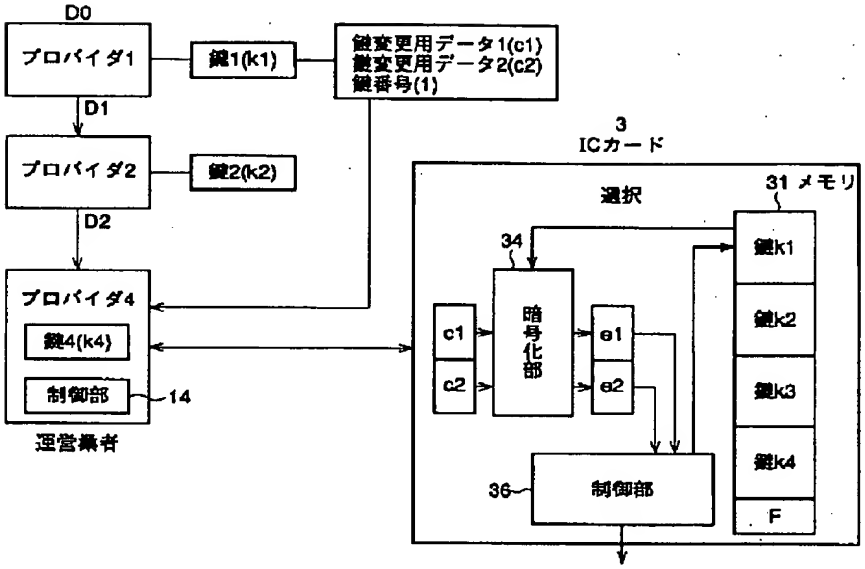
【図１６】


1 コントローラ
2 リーダライタ
3 ICカード
12
通信部
K4
22
暗号化部
21
通信部
縮退鍵
211
ID取得部
24
制御部
縮退順序
D_{012},K4
11 メモリ
D_{012},K4
縮退順序
14
制御部
23
乱数生成部
(プロバイダ4)
相互認証
36
制御部
33
通信部
縮退鍵
201
ID番号
35
乱数生成部
34
暗号化部
32
鍵の縮退処理部
秘密データ
D_0
暗号鍵1
エリア1
暗号鍵2
エリア2
暗号鍵3
エリア3
暗号鍵4
エリア4
暗号鍵5
エリア5
暗号鍵6
エリア6
31 メモリ

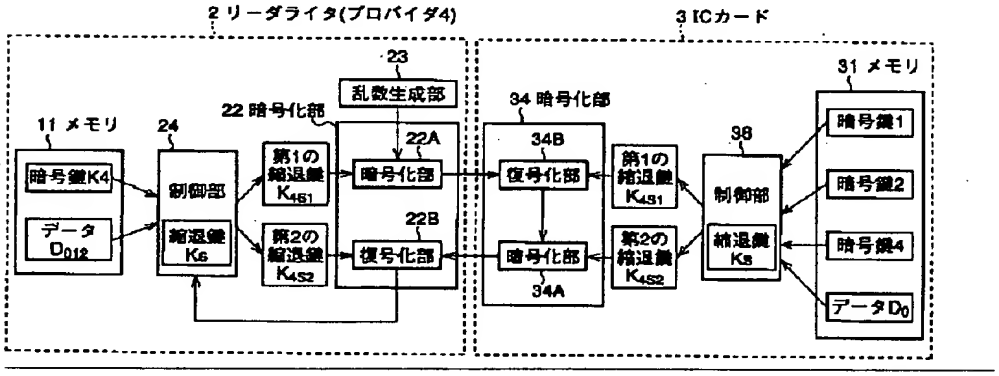
【図１７】


2
3A
3B
リーダライタ
ICカードA
ICカードB
S41
ID要求
S42
乱数発生
S45
乱数発生
S43
タイムスロット割当
S46
タイムスロット割当
S44
IDA
S47
IDB
S48
乱数r1生成
S49
D012,IDA,K4
から縮退鍵生成
S50
プロバイダ数
プロバイダ番号
縮退順序、乱数r1
S51
K1,K2,IDB,K4
から縮退鍵生成
S52
k1,k2,IDA,k4から縮退鍵生成
S53
乱数r1を縮退鍵で暗号化→R1
S54
乱数r2生成
S55
R1,r2
縮退鍵でR1を復号→r1をチェック
S56
r2を縮退鍵で暗号化→R2
S57
S58
R2
R2を縮退鍵を用いて復号→r2をチェック
S59

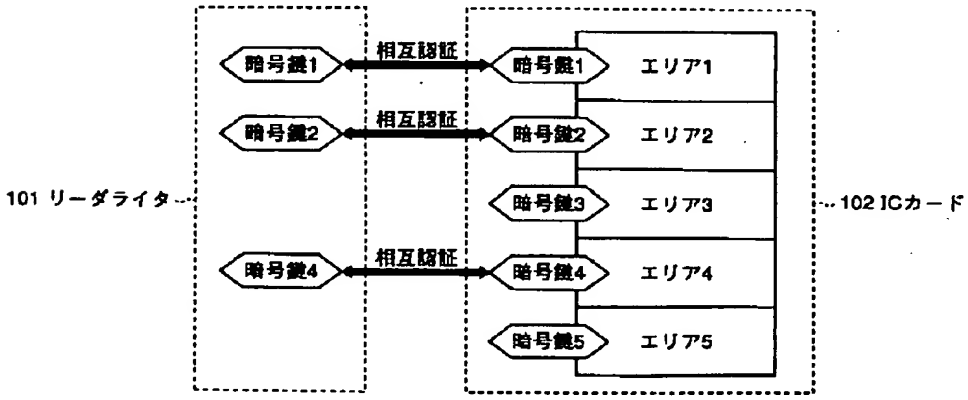
【図１８】


D0
プロバイダ1
鍵1(k1)
鍵変更用データ1(c1)
鍵変更用データ2(c2)
鍵番号(1)
D1
プロバイダ2
鍵2(k2)
D2
プロバイダ4
鍵4(k4)
制御部
14
運営業者
3
ICカード
選択
31 メモリ
34
暗号化部
c1
c2
e1
e2
鍵k1
鍵k2
鍵k3
鍵k4
F
36
制御部

【図１９】


2 リーダライタ(プロバイダ4)
3 ICカード
23
乱数生成部
22 暗号化部
22A
22B
暗号化部
復号化部
11 メモリ
暗号鍵K4
データ D012
24
制御部
縮退鍵 K6
第1の縮退鍵 K451
第2の縮退鍵 K452
34 暗号化部
34B
復号化部
暗号化部
34A
第1の縮退鍵 K451
第2の縮退鍵 K452
38
制御部
縮退鍵 K6
31 メモリ
暗号鍵1
暗号鍵2
暗号鍵4
データ D0

【図２０】


101 リーダライタ
102 ICカード
暗号鍵1
相互認証
暗号鍵1
エリア1
暗号鍵2
相互認証
暗号鍵2
エリア2
暗号鍵3
エリア3
暗号鍵4
相互認証
暗号鍵4
エリア4
暗号鍵5
エリア5